

Department of Health and Human Services

Privacy Manual

**Prepared by the DHHS Privacy
and Security Office**

Publication Date:

October 7, 2015

DHHS is entrusted with millions of documents containing confidential personal and health information of its program recipients, clients and workforce members. The HIPAA Privacy Rule requires that HIPAA-covered DHHS agencies implement appropriate administrative, physical, and technical safeguards to avoid the unauthorized use or disclosure of their protected health information. In order to ensure that all forms of confidential information are protected, DHHS also requires its agencies that use, collect, disclose, or store confidential information to implement these same three types of safeguards. The purpose of the privacy manual is to offer a guide for the North Carolina Department of Health and Human Services (NC DHHS) divisions, facilities and schools as they work towards protecting their citizens.

The federal standards for privacy of individually identifiable health information final rule (hereinafter referred to as the HIPAA privacy rule), promulgated to implement the Health Insurance Portability and Accountability Act (HIPAA), made significant changes in the protection of certain individually identifiable health information that is created, received, transmitted and maintained in any form or medium, by the DHHS. Health care providers and health care plans within DHHS that perform specific electronic transactions must comply with the HIPAA regulations. These divisions, facilities and schools (or portions thereof) shall be known as “covered health care components” throughout this manual.

The NC Office of Attorney General has determined that DHHS meets the definition of a “hybrid entity” and has both covered health care components and non-covered health care components within its department. DHHS, as a hybrid entity, is responsible for designating which of its divisions and offices are covered health care components and for ensuring that those components comply with HIPAA.

The department shall ensure compliance with privacy and confidentiality requirements through the development and implementation of privacy guidelines that specify the Department's methods for the protection of Protected Health Information (PHI), Personally Identifiable Information (PII) and any other confidential information. The requirements in these policies shall be based on many business practices already employed by DHHS divisions, facilities and schools. In addition, privacy policies shall include other federal and state law requirements that have an impact on the use and disclosure of health information. Most federal and state laws that are more stringent than the HIPAA requirements will generally remain in effect and will not be preempted by HIPAA. In addition, some state laws such as categories of laws that provide for reporting of disease or injury, child abuse, birth or death and other laws requiring disclosure of individually identifiable health information will remain in effect.

The department shall modify, in a prompt manner, its privacy policies as necessary and appropriate to comply with changes in the state and federal law and ongoing business practices. Changes to policies may be made at any time, provided such changes are documented and implemented according to DHHS policy requirements. DHHS offices shall modify, in a prompt manner, their individual privacy procedures to conform to revised department privacy policies

DHHS divisions, facilities and schools may only use and disclose individually identifiable health information as provided in this document and are subject to all of the limitations and requirements specified in this manual.

TABLE OF CONTENTS

Chapter 1: Privacy Safeguards	9
Chapter 2: Incident and Complaint Reporting	17
Chapter 3: Identity Theft Red Flags et al.	21
Chapter 4: Identity Theft and Security Breach Notification	35
Chapter 5: Notice of Privacy Practices	38
Chapter 6: HIPAA Violation Sanctions	44
Chapter 7: Privacy Official	45
Chapter 8: Workforce	47
Chapter 9: Business Associates	50
Chapter 10: Legal Occurrences	55
Chapter 11: Authorizations	61
Chapter 12: Consent for TPO	65
Chapter 13: Use and Disclosure	67
Chapter 14: Accounting of Disclosures	87
Chapter 15: De-Identification of Health Information & Limited Data Sets	95
Chapter 16: Minimum Necessary	104
Chapter 17: Research	107
Chapter 18: Marketing and Fundraising	116
Chapter 19: Rights of Clients	118
Chapter 20: Personal Representatives	130

Chapter 21: Designated Record Sets	134
Chapter 22: Acceptable Use for DHHS Information System	138

DEFINITIONS

Please note that this is not an inclusive list. Some definitions are being included for your convenience.

Access: the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach: the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

Business: A sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit. The term includes a financial institution organized, chartered, or holding a license or authorization certificate under the laws of this State, any other state, the United States, or any other country, or the parent or the subsidiary of any such financial institution. Business shall not include any government or governmental subdivision or agency (See N.C.G.S. § 75-61).

Business associate: An entity that performs functions, activities or services on behalf of covered entities that involve use or disclosure of PHI. Business associates may “create, receive, maintain or transmit” PHI, clarifying that entities that store PHI are now business associates. Subcontractors of business associates are also now considered business associates.

Collect: To request SSNs and other identifying information from a DHHS client or workforce member utilizing a paper document or a DHHS system application.

Confidential information: Information that is “non-public” or deemed confidential by state or federal law (i.e., state statute, administrative code, federal regulation, etc.), including SSNs and other identifying information, PHI, tax records, client program eligibility information, etc.

Covered entity: a health plan, health care clearinghouse, or health care provider that transmits any health information electronically in connection with a covered transaction, such as submitting health care claims to a health plan.

Device: Computers and any other equipment or devices that store or display data including, but not limited to the following: PDAs, smartphones (Treos, Blackberry, Palm devices), copiers, printers, disk drives, diskettes, CDs, or USB (thumb) drives.

Disclose: To communicate or make available SSNs, other identifying information, or documents containing SSNs or other identifying information to third parties using verbal, written, or electronic means.

Discovered: the first day on which the breach is known to a HIPAA-covered DHHS agency, or would have been known to any person who is a workforce member by exercising reasonable diligence.

Encryption: The use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key (See N.C.G.S. § 75-61(8)).

HIPAA Privacy Rule: The HIPAA Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether **electronic, paper, or oral**. The HIPAA Privacy Rule calls this information PHI.

Identifying Information: N.C.G.S. § 14-113.20(b) includes all of the items listed below.

- SSNs or employer identification numbers (EINs)
- Drivers license, state identification card, or passport numbers
- Checking and savings account numbers
- Credit and debit card numbers
- Personal Identification Number (PIN) code, as defined in N.C.G.S. § 14-113.8 (6)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Biometric data
- Fingerprints
- Passwords
- Parent's legal surname prior to marriage.

However, with regard to N.C.G.S. § 132-1.10, "**identifying information**" does not include the items below:

- Electronic identification numbers, electronic mail names or addresses, Internet account numbers, Internet identification names,
- Parent's legal surname prior to marriage, or
- Drivers license numbers appearing on law enforcement records (See N.C.G.S. § 132-1.10(b)(5)).

Individual: A DHHS state employee, contractor, or volunteer or a client receiving services provided by DHHS. **Individually identifiable health information:** information that is a subset of health information, including demographic information collected from an individual, and:

- Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
- Relates to the past, present, or future physical or mental health or condition of an Individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
 1. Identifies the individual; or
 2. Reasonably could be used to identify the individual.

Law enforcement official: an officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, who is empowered by law to:

- Investigate or conduct an official inquiry into a potential violation of law; or

- Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Limited data set: protected health information that excludes the following direct identifiers of the individual or of relatives, employers, or household members of the individual: (1) Names; (2) postal address information, other than town or city, State, and zip code; (3) telephone numbers; (4) fax numbers; (5) e-mail addresses; (6) social security numbers; (7) medical record; (8) health plan beneficiary numbers; (9) account numbers; (10) certificate/license plate numbers; (11) vehicle identifiers and serial numbers; (12) device identifiers and serial numbers; (13) Web URLs; (14) Internet Protocol (IP) address numbers; (15) biometric identifiers, including finger and voice prints; and (16) full face photographic images and any comparable images.

Non-DHHS Organization: A government or governmental subdivision or agency, federal or state, and any "business" as defined above.

Personal Information: A person's first name **or** first initial **and** last name in combination with "identifying information," as defined above in N.C.G.S. § 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records (See N.C.G.S. § 75-61(10)).

Privacy complaint: An allegation made by an individual that there has been an unauthorized access to, or the use, disclosure, and/or collection of, confidential information.

Privacy incident: An event or action resulting from the unauthorized access, use, disclosure, or collection of confidential information.

Protected health information: individually identifiable health information that is:

- Transmitted by electronic media;
- Maintained in electronic media; or
- Transmitted or maintained in any other form or medium.

Excludes individually identifiable health information in:

1. Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;
2. Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and
3. Employment records held by a covered entity in its role as employer.

Redaction: The rendering of data so that it is unreadable or is truncated so that no more than the **last four (4) digits** of the identification number is accessible as part of the data (See N.C.G.S. § 75-61(13)).

Risk Assessment: a document that DHHS agencies must complete when submitting a privacy incident or complaint electronically. This document's questions help DHHS agencies determine whether there has been a breach of unsecured PHI.

Security Breach: An incident of unauthorized access to and acquisition of unencrypted and un-redacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to an individual. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the department for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure (See N.C.G.S. § 75-61(14)).

[Security] Incident: A violation of DHHS computer security policies, acceptable use policies, or standard computer security practices. An adverse event where a NC information technology resource is accessed or used without authorization, attacked or threatened with attack, or used in a manner inconsistent with established policy with the potential to cause the real or possible loss of confidentiality, integrity, or availability of the resource or its information (See NC DHHS Policies and Procedures Manual, Section VIII - Privacy & Security - Security Manual – Glossary Policy).

Store: To maintain SSNs and other identifying information in a system application or keep documents containing SSNs and other identifying information in a locked file cabinet for future access and use.

Use: To utilize SSNs and other identifying information for some DHHS business purpose.

Workforce member: employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

DHHS must establish privacy safeguards that protect individually identifiable health information from unauthorized use or disclosure and to further protect such information from tampering, loss, alteration, or damage. It is not the intent of this policy to address all of the safeguards necessary to protect electronic data containing individually identifiable health information since those safeguards are included in the Department of Health and Human Services (DHHS) Security Policies.

The policy is applicable to all DHHS agencies that deal with individually identifiable health information (IIHI), regardless of whether they are a Covered component, an Internal Business Associate or a Non-covered health care component.

The HIPAA Privacy Rule requires covered health care components to implement appropriate administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of individually identifiable health information. Agencies are not asked to “guarantee” the safety of individually identifying health information against all imaginable assaults; instead, agencies are instructed to use protections that are flexible, scalable, and provide reasonable safeguards. The safeguards implemented in different DHHS agencies will vary depending on factors such as agency size and the nature of its business. To implement reasonable safeguards, each agency should analyze its own needs and circumstances such as the nature of the information it holds, and assess potential risks to a client’s privacy. DHHS agencies should also consider the potential impacts on client care and other issues such as the financial and administrative burdens of implementing various safeguards.

Safeguards addressed in DHHS Privacy Policies include the administrative, physical, and technical protections necessary for safeguarding individually identifying health information as it is found in the working environment (e.g., oral communications, paper records, medical supplies/equipment, computer screens, etc.).

DHHS has determined that the requirement to safeguard confidential health information should be extended to all agencies within the department that maintain individually identifiable health information.

Administrative Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each agency. Confidential information that is transmitted by facsimile (fax) machines, e-mail, printers, copiers, and by telephone or other oral means of communication shall be protected from unauthorized use and disclosure. DHHS agencies shall address measures to direct the conduct of agency staff in relation to the protection of individually identifiable health information; and develop and implement appropriate agency safeguard procedures.

Authorized Disclosures of Individually Identifiable Health Information

Disclosure of individually identifiable health information is essential to health care providers and health plans for a variety of reasons including treatment, payment of health care services, or health care operations (TPO) purposes. Safeguarding such information requires agencies to ensure the following prior to disclosure:

- The disclosure is permitted for TPO;
- The disclosure is authorized by the client;
- The disclosure does not violate a communications or use and disclosure restriction that the client has requested and the agency has granted; or
- The disclosure is required or permitted by law.

DHHS agencies shall develop and implement procedures that ensure that chosen methods of disclosing individually identifiable health information outside the agency are safeguarded to protect client confidentiality.

MAIL OR HAND DELIVERY

Whenever feasible, documents containing individually identifiable health information should be hand delivered or mailed using the United States Postal Service (USPS), courier, or other delivery service. All documents containing individually identifiable health information shall be placed in a secure container (e.g., sealed envelope, lock box) that is labeled "Confidential", addressed to the recipient, and include a return name and address. When transmitting individually identifiable health information via interoffice mail, the information shall be placed in a sealed envelope and then placed in an interoffice envelope.

DHHS agencies must designate specific fax machines that will be used to send and/or receive documents containing individually identifiable health information. Where possible, fax machines should be strategically located near the intended recipient(s) of the health information.

Incoming fax transmissions of documents that contain individually identifiable health information must be protected from unauthorized disclosure to staff or others who are not authorized to access the information. Each agency must determine the methods to be used in that agency to ensure the protection of incoming individually identifying health information via fax transmission. Staff should request that those faxing confidential information to the agency call in advance to schedule the transmission.

- Efforts to protect outgoing fax transmission of documents containing individually identifiable health information shall be initiated by agency staff as listed below.
- Prior to faxing such documents, agency staff shall attempt to schedule the transmission with the recipient so that the faxed document can be promptly retrieved by the recipient.
- Whenever feasible, routine destination fax numbers should be pre-programmed into fax machines. DHHS agencies shall test pre-programmed numbers at regular intervals (e.g., monthly) to reduce transmission errors.
- Agencies should request that routine recipients of faxed documents containing IIHI inform the agency immediately if their fax number(s) change so that agency records and pre-programmed numbers can be updated accordingly.
- Staff authorized to send faxes with individually identifiable health information shall check the recipient's fax number before transmittal and shall confirm delivery via telephone or review of the confirmation sheet of fax transmittal.

- Agencies shall implement procedures for maintaining and reviewing fax transmittal summaries and confirmation sheets.
- In the event of a misdirected fax, the recipient must be contacted immediately and shall be asked to destroy the information by burning or shredding the document. Misdirected faxes are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report.
- DHHS agencies shall include a confidentiality statement on all fax cover sheets.

In addition to the required confidentiality statement, the fax cover sheet should contain:

- Sender's name, mailing address, e-mail address, telephone number, and fax number;
- Recipient's name, telephone number, and fax number;
- Number of pages transmitted, including coversheet; and
- Instructions for verification of fax receipt (e.g., phone call to sender to confirm receipt of the document).

EMAIL

Emails containing individually identifiable health information should be both encrypted and password protected. An automatic delay should be placed on all employee and staff email systems forcing the emails to wait in queue prior to being sent.

DHHS agencies need to be aware that:

- Email is considered public record but confidential information contained in or attached to an e-mail can be protected from public disclosure in accordance with NCGS 132-6(c).
- E-mails containing individually identifying health information can be forwarded by the recipient to someone not authorized to have access to the information; therefore, DHHS agencies shall only transmit e-mails containing individually identifiable health information to persons within DHHS who are knowledgeable about DHHS Privacy Policies, to business associates, or to other covered entities (e.g., health plans, health care providers).
- All efforts should be made to avoid using e-mail for particularly sensitive matters (e.g., HIV status, psychiatric disorders) and time-sensitive messages (e.g., appointment scheduled for next day).
- Avoid including individually identifiable health information in the subject line or body of an e-mail. If it is essential for the efficiency of business operations to send individually identifiable health information via e-mail, the information must be sent as a password protected attachment to the e-mail. Agencies are discouraged from using direct identifiers in the attached document (e.g., client name, social security number, address) and should de-identify the information whenever feasible.
- In accordance with the State of North Carolina (NC) Enterprise Security Standard, S002, passwords shall not be inserted into e-mail messages or other forms of electronic communication without proper encryption. Passwords for e-mail attachments shall be

provided to recipients in a secured manner (e.g., by phone, fax, or pre-assigned passwords provided to a receiving agency).

- Tracking numbers for Incidents should not be sent via email.
- Ensure that e-mails are addressed correctly by reviewing the recipient's e-mail address before sending the e-mail to ensure that the e-mail software did not automatically fill-in an incorrect e-mail address after the first few characters of the address were typed.
- When disclosing individually identifying health information to a third party for purposes other than treatment, payment, or health care operations, the disclosure must be documented and accounted for.
- In the event of a misdirected e-mail with a file attachment that contains individually identifying health information, the recipient must be contacted immediately and shall be asked to delete the e-mail and attachment. Misdirected e-mails are considered accidental disclosures and must be accounted for in accordance with DHHS Privacy Policy, Use and Disclosure Policies, Accounting of Disclosures. In addition, the agency shall complete a Privacy Incident Report in accordance with DHHS Privacy policies.

DHHS agencies shall include a confidentiality statement on all e-mails containing individually identifiable health information as file attachments.

Telephone

Whenever it is necessary for agency staff to discuss individually identifiable health information via the telephone with a client or a client's family members/friends, agency workforce members, business associates, other health care providers, or health plans, staff must follow the agency's requirements for protecting such information.

Each agency shall develop and implement procedures for identifying individuals to whom a specific client's health information may be released via the telephone. Each agency shall honor any agreed upon requests made by the client as to the use of alternate forms of communication (e.g., alternate telephone numbers) or restrictions regarding the use or disclosure of that clients individually identifying health information. Agency procedures must include the stipulation that telephone conversations that include the use or disclosure of confidential information be conducted in private locations wherever possible and in a soft voice to ensure such information is shared with only the intended recipient.

Agency staff shall not discuss individually identifiable health information (e.g., client's diagnosis or condition) until the following can be confirmed:

- Identity of the caller (e.g., a "call back" to validate the number called or voice recognition) and
- Verification that the caller has a need to know, and the use or disclosure of confidential information is permissible.
- If confirmation cannot be made, the agency shall neither confirm nor deny that the client has in the past or is currently receiving services from the agency. The caller's information can be recorded and provided to the client for disposition.

Agency procedures should also include the following practices for making calls:

- Agency staff shall not discuss individually identifiable health information until the identity of the person on the phone line has been confirmed. This may be accomplished through voice recognition or call-back.
- In the event an answering machine/voice mail system picks up the call, staff should leave a message requesting that the person they need to speak to return the call. The message shall include **ONLY** the name and telephone number of the person that should receive the return call (e.g., "This message is for Mary Jones. Please contact Mary Smith at 555-1313"). Messages left on an automatic answering machine or voice mail system shall not contain confidential health information (e.g., name of the client, diagnosis, test results).

Agency staff shall be informed of the security risks of cellular/wireless phones. Communication via cellular and wireless phones should not be used to discuss confidential information; this communication is not secure, unless encrypted. Agency staff shall not use these devices to communicate confidential information unless there is an emergency and a wired, landline phone is not readily available.

DHHS agencies must take reasonable steps to protect the privacy of all verbal exchanges or discussions of individually identifying health information, regardless of where the discussion occurs. Where possible, each agency shall make enclosed offices and/or interview rooms available for the verbal exchange of individually identifying health information.

In work environments that contain few offices or closed rooms, DHHS staff participating in the verbal exchanges of individually identifying health information shall conduct these conversations in a soft voice and as far away from others as possible.

Physical Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, transmitted and/or maintained throughout each agency by establishing protections used for equipment/supplies/records/work areas to prevent unauthorized use or disclosure of individually identifiable health information maintained by the agency.

A physical safeguards assessment shall be conducted and the associated documentation maintained by each agency to demonstrate due diligence in complying with DHHS physical safeguards requirements. The information collected will assist each agency in determining where physical safeguard deficiencies exist and in identifying the measures necessary to secure the area. Agencies shall identify in their procedures the frequency and/or circumstances (e.g., office relocations or agency reorganizations that result in changes in the security of individually identifiable health information) that would require a review and updated physical safeguards assessment.

Each agency shall identify those areas wherein agency staff routinely maintain, transmit, and receive individually identifiable health information on paper, biomedical equipment, or other non-electronic medium (e.g., prescription bottles, test tubes, specimen vials). Agencies must ensure these areas are routinely manned or physically secured as appropriate during business and non-business hours and that such areas are accessed only by authorized staff. Securing confidential information may be as simple as employing locks on file cabinets, safes, and desk drawers or as complex as relocating equipment or an entire work area to a more secure location.

Each agency shall develop and implement procedures for limiting physical access to individually identifiable health information maintained throughout the agency while ensuring that properly authorized access is allowed. Physical security of health information is most vulnerable in the following areas:

- Client records storage areas;
- Shared office areas containing faxes, copiers, and printers; and
- Open work areas or workstations.

Areas that use white boards, chalk boards, posters, etc. must be evaluated to ensure individually identifiable health information is not displayed or unintentionally disclosed through these devices. For example, agencies may develop the following procedures:

- Post client first name and last initial (or vice versa) on boards.
- Cover information identifying clients with a cover sheet.
- When a client's record is placed in a bin outside an examination/treatment room, position the record so that the client's name is not visible.

Biomedical devices such as electrocardiograph machines and medical imaging systems must be safeguarded from unauthorized access if they display memory, connect to another system, or transfer data.

Each agency shall maintain documentation of building repairs, workspace modifications, and equipment purchases that are instituted to cure physical safeguard deficiencies. Such records will serve as documentation of due diligence.

DHHS agencies shall ensure that observable individually identifying health information displayed on computer screens is adequately shielded from unauthorized disclosure. Agencies shall safeguard individually identifiable health information displayed on computer monitors by:

- Relocating the workstation or repositioning the computer monitor so only the authorized user can view it;
- Installing polarized screens (also referred to as privacy or security screens) or other computer screen overlay devices that shield information on the screen from persons who are not directly in front of the monitor; and
- Clearing information from the computer screen when it is not actually being used, turning off computer when not in use, or by activating a password-protected screen-saver.

Each agency shall take reasonable steps to ensure the privacy of client information in treatment areas and other areas in the agency where visitors, repairmen, vendors, and family members are permitted. General safeguards shall include measures the facility has implemented that protect individually identifiable health information from unauthorized use or disclosure.

Facility Safeguards include the following:

- Sign-in Sheets - Ensure sign-in sheets that are viewed by multiple clients do not contain health information and unnecessary identification information
- Client/Staff Conversations - Establish precautions to prevent conversations regarding client information from being overheard by others. Designate an area away from waiting areas to have conversations involving confidential information. Intercom - Limit information given over an intercom system. For example, do not instruct specific clients to report to a certain testing or procedure area.
- Treatment Areas - Limit access to treatment areas. Individuals that are not essential workforce members (e.g., clients, family members, drug reps) should be escorted in all treatment areas.
- Client Records - Assure clients records used in treatment areas are reasonably protected to prevent inadvertent disclosures. For example, place a cover sheet over records sitting on a desk or position a client's record so that the client's name is not visible. Maintain client records in secure area. (e.g., locked office/nursing station, locked file cabinet).

Visitor Safeguards should include:

- Sign-in Logs - Ensure sign-in logs are used that record the visitor's name, company, area visited, time in, and time out.
- Badges - Provide visitors with identification badges.
- Escort - Establish procedures for when visitors must be escorted within the agency. Unescorted visitor access should be limited to those areas that do not contain individually identifying health information.

Each agency shall establish a process for safely disposing of paper and other materials containing individually identifiable health information. Paper records include, but are not limited to, client records, billing records, and correspondence. Other materials include, but are not limited to, client consumables and non-durable medical equipment such as x-ray films, identification bracelets, identification plates, IV bags, prescription bottles, syringes, diskettes, disk drives, etc. It is recommended that, where practical and when permitted, paper materials containing individually identifiable health information be shredded or burned. All steps in the shredding or burning process shall be protected, including any shred/burn boxes, bins, and bags containing individually identifying health information to be destroyed.

Allowing DHHS workforce members to remove individually identifying health information from a DHHS agency premises for purposes other than treatment or in response to a court order, or allowing workforce members to access individually identifiable health information outside of the secured work environment, is strongly discouraged. However, it is recognized that there may be circumstances where work outside of the secured environment. DHHS agencies shall develop and implement procedures to ensure the security of confidential information taken outside the secured work environment, including, but not limited to, the following guidelines.

- Ensure privacy and security of remote work area;
- Restrict telephone conversations to a private area using a wired, landline phone;

- Ensure faxed documents are handled according to the guidelines in this policy; and
- Secure confidential information in locked rooms or locking storage containers (e.g., filing cabinets, safes, desk drawers) when not in use.

Original client medical or financial records in paper format shall never be removed from the DHHS agency responsible for safeguarding the records unless under order of the court or when necessary for treatment purposes (which includes autopsies).

Technical Safeguards

DHHS agencies shall safeguard individually identifiable health information that is generated, received, and/or maintained throughout each agency by addressing technical safeguards used for accessing confidential information maintained in computer systems and other electronic media through identification of staff who need access to electronic data and control of access through the use of unique user identifiers and passwords.

Each agency shall determine which workforce members, or classes of workforce members based on job responsibility, require access to individually identifiable health information. Privileges shall be established on a "need to know" basis for each user relative to their specific relationship with clients and specified business needs for accessing individually identifiable health information. It will be the responsibility of each agency to determine the level of individually identifiable health information detail a workforce member can access, such as an entire record, department files, individuals' files, workstation, software applications, electronic data, electronic report files (e.g., X/PTR), etc. The access level of individually identifiable health information granted to an individual shall be the minimum necessary needed to do his/her job.

DHHS agencies shall require its staff to use personal passwords in situations determined appropriate by the agency. Agencies shall develop procedures to ensure passwords are protected and define situations or circumstances when a supervisor or other designated staff may have access to a user's password. In special cases where a user is required to divulge his/her personal password such as for system support, the user shall immediately change the password.

Passwords shall not be included in e-mail messages or unencrypted computer files; nor shall passwords be stored in a location readily accessible to others. Agencies shall require staff with access to individually identifiable health information to change their password at least every 90 days or immediately if the security of a password has been jeopardized.

Additional information regarding password protections can be found in the ITS Statewide Information Security Manual.

Chapter 2: Incident and Complaint Reporting

DHHS agencies shall immediately report, investigate, and document all suspected privacy incidents or complaints electronically to the Privacy and Security Office Incident Reporting Tool, ensuring that all required documents are attached to the electronic report. The reporting tool can be found at:

<http://www.ncdhhs.gov/psa/incidents.htm>

There are a variety of federal laws that we need to follow, with regards to breach notifications. It is imperative that the PSO learns of any potential breach as soon as possible, so an investigation can be started. If it is necessary to report a suspected breach to a federal organization, the PSO will need to be alerted as quickly as possible, so they may do so in a timely manner. For example, in the event of a breach of social security numbers provided by the Social Security Administration (SSA), the Department must alert the SSA within **60** minutes of becoming aware of the incident.

Incidents include suspected violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the North Carolina (NC) Identity Theft Protection Act, SSA data and/or the department's privacy practices, policies or procedures regarding confidential information. DHHS agencies shall respond to every identifiable privacy incident or complaint received. Each identifiable privacy incident or complaint shall generate an investigation, determination and a response. Ensuing investigations should focus on both the specific privacy incident or complaint and any patterns of similar privacy incidents or complaints.

Documentation of privacy incidents or complaints, investigative efforts, and incident or complaint determinations are considered administrative information and shall be maintained in administrative files for at least six (6) years. If a client who should receive a breach notification letter cannot be located, that letter should be placed in their treatment folder.

Each agency shall designate a staff member who is responsible for communicating and assisting workforce members or individuals who have questions or concerns, or who wish to file incidents or complaints regarding the agency's privacy practices. Both privacy and security incidents and/or complaints should be reported via the online incident reporting tool.

When reporting incidents or complaints electronically, the agency shall report its internal incident or complaint number, incident classification and severity, investigative analysis of the facts, description of the corrective actions taken, and mitigation efforts undertaken. The report shall be updated using the ticket tracking ID number, which is generated after submitting the incident or complaint until the investigation is completed and closed. In addition, any privacy incident or complaint that includes a disclosure for which an accounting is required must be documented and entered into the accounting of disclosures logs. This staff member will make every effort to respond to communications from the PSO in a timely manner.

Each agency shall determine its procedures for investigating and resolving privacy incidents or complaints. However, each agency must designate an individual as *Privacy Official* (if covered by HIPAA) and/or as *Privacy Coordinator* (if not covered by HIPAA), who will be responsible for reporting, investigating and documenting privacy incidents or complaints.

If an individual contacts the agency directly, the agency's Privacy Official or Privacy Coordinator shall determine if the issue can be resolved at the agency level. If so, the Privacy Official or Privacy Coordinator shall be responsible for investigating and documenting the concern until the issue is resolved. Agencies operated by the Division of State Operated Healthcare Facilities are encouraged to involve their internal client advocates in the complaint investigation process when deemed appropriate.

If the Privacy Official or Privacy Coordinator determines the issue involves other agencies in the department or if he/she is unable to obtain resolution at the agency level, the issue shall be forwarded to the DHHS Privacy and Security Office.

The DHHS Privacy and Security Office shall review the reporting, documentation and resolution of all privacy incidents or complaints. If the agency has not resolved the incident within a reasonable time, the DHHS Privacy and Security Office shall involve anyone determined to be necessary to assist in resolution of the incident or complaint, including the Attorney General's Office. If the DHHS Privacy and Security Office has comments, suggestions, questions, etc. about the investigation and resolution of the incident or complaint, he or she shall document this information within the report for consideration by the agency.

When completing the Incident Reporting form, all attempts should be made to answer as many of the following questions as is possible, where relevant. If all the answers are not known, the ticket should still be opened, and the privacy officer should work on collecting the following information. Was health or financial information involved;

- What types of information was lost or stolen?
- Was the individual's first name **or** first initial **and** last name included;
- Was the identifying information in electronic or paper form;
- Was the information or the laptop encrypted (128-bit encryption);
- Was the identifying information stolen, lost, misplaced or other; and
- Was the information disclosed to the public?

Once reported, the DHHS PSO, in conjunction with the DHHS agency's Privacy Official or Privacy Coordinator and other necessary staff, will make an initial evaluation to determine the following:

- If the matter should be reported to the NC Office of Technology Services (ITS) as a [security] incident;
 - If the disclosure or potential disclosure involved confidential information;
 - If the disclosure or potential disclosure involved protected health information or electronic protected health information; and
 - If the disclosure or potential disclosure involved unencrypted and unredacted records or data containing "personal information".
-
- Was health or financial information involved;
 - Was the individual's first name **or** first initial **and** last name included;
 - Was the identifying information in electronic or paper form;
 - Was the information or the laptop encrypted (128-bit encryption);

- Was the identifying information stolen, lost, misplaced or other; and
- Was the information disclosed to the public?

After notifying the DHHS agency about the incident, DHHS agencies should require that the non-DHHS organization complete a risk assessment immediately, but no later than five (5) business days, to determine whether there has been a "security breach." If definite answers to all of the questions above are not available at the time the incident is reported, the non-DHHS organization shall provide the remaining answers as they become available. The burden to determine whether there is a risk of harm resulting from the breach is on the DHHS agency - not the non-DHHS organization. Therefore, a non-DHHS organization **should not** have the discretion to determine whether notification will occur.

Often times, a privacy breach is entwined with a security breach. N.C.G.S. § 132-1.10(c1) specifically states that if an agency of the State or its political subdivisions, or any agent or employee of a government agency, experiences a security breach, the agency shall comply with the requirements of N.C.G.S. § 75-65. Accordingly, DHHS agencies are obligated to notify the Consumer Protection Division of the Attorney General's Office pursuant to N.C.G.S. § 75-65(e1), without unreasonable delay, when there is a security breach and notice to affected persons is required. DHHS agencies shall complete the "North Carolina Security Breach Reporting Form" on the NC Attorney General's Office's website at <http://www.ncdoj.gov/getdoc/81eda50e-8feb-4764-adca-b5c47f211612/Report-a-Security-Breach.aspx> and ensure that they include the following information in the form:

- nature of the breach,
- the number of consumers affected by the breach,
- steps taken to investigate the breach,
- steps taken to prevent a similar breach in the future, and
- information regarding the timing, distribution, and content of the notice

DHHS General Counsel will handle notification to the Consumer Protection Division of the NC Attorney General's Office.

Duty to Report to both the Attorney General's Office and Consumer Reporting Agencies:

N.C.G.S. § 75-65(f) requires that in the event DHHS provides notice of a security breach to more than 1,000 persons at one time, it shall notify, without unreasonable delay, the Consumer Protection Division of the NC Attorney General's Office and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C. § 1681a(p), of the timing, distribution, and content of the notice.

If more than 1,000 affected persons at one time must be notified, DHHS agencies shall follow the procedure outlined in Section D above and report the security breach to the three credit reporting agencies, Equifax, TransUnion, and Experian.

Equifax Fraud Division
P.O. Box 740250
Atlanta, GA 30374

(800) 525-6285

Website: www.equifax.com

Experian Fraud Division

P.O. Box 1017

Allen, TX 75013

888-397-3742

www.experian.com

TransUnion Fraud Division

P.O. Box 6790

Fullerton, CA 92634

800-680-7289

www.transunion.com

Duty to Report to the General Assembly

N.C.G.S. § 120-270 requires all agencies of the state to evaluate and report to the General Assembly about the agency's efforts to reduce the dissemination of identifying information, as defined in N.C.G.S. § 14-113.20(b) by December 31st of each year. The evaluation includes a review of the agency's public forms, the use of its random personal identification numbers, the restriction of access to its personal identifying information, and the reduction of use of its personal identifying information when it is not necessary. Special attention should be given to the agency's use, collection, and dissemination of SSNs.

In order to ensure compliance with this statute, the DHHS PSO shall coordinate the evaluation and reporting of the department's efforts to reduce the dissemination of SSNs and other identifying information. With the exception of the DHHS PSO, the Office of the General Counsel, and the NC Office of Public Affairs, DHHS workforce members **are not** authorized to speak on behalf of the department to media personnel or representatives of other outside agencies concerning privacy or security incidents.

DHHS agencies shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident or a complaint.

Chapter 3 Identity Theft Red Flags and Address Discrepancy Policy

In response to the growing identity theft trends, industry regulators amended the Fair and Accurate Transactions Act of 2003 to include Identity Theft Red Flags and Address Discrepancy requirements. This requires financial institutions, creditors which own or maintain covered accounts, and debit or credit card issuers (debit/credit card issuers) to develop and implement certain programs and procedures.

The Red Flags and Address Discrepancy Rules have a broad applicability. Although one would not ordinarily think of divisions or offices operating as a financial institution, a creditor, or a debit/credit card issuer within the meaning of the Rules, divisions and offices do offer services and programs that can meet one or more of these categories.

In order for a division or office to officially determine whether it must comply with the Red Flags and Address Discrepancy Policy requirements, it must first assess whether it operates as a *financial institution*, a *creditor that offers or maintains covered accounts* and/or a *debit/credit card issuer*. If the division or office determines that it meets the definition of either of these three (3) categories, it must perform a risk assessment and develop the required procedure(s).

DEFINITIONS

An **account** is a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes: An extension of credit, such as during the purchase of property or services involving deferred payment.

A **cardholder** is a [client] who has been issued a debit or credit card.

The term **clear and conspicuous** means reasonably understandable and designed to call attention to the nature and significance of the information presented.

A **client** is an individual that receives services from programs offered by NC DHHS divisions and offices. For the purposes of this policy, a client can be considered a consumer who acquires services for direct use, including but not limited to any form of monetary benefit.

A **consumer reporting agency** is defined under the Fair Credit Reporting Act (FCRA) as any entity “which for monetary fees, dues or on a cooperative, non-profit basis regularly engages . . . in the practice of assembling or evaluating consumer credit information or other information on consumers.” It does not include governmental agencies or public law enforcement authorities. The extremely broad definition does include, however, private security firms hired by employers to conduct background checks and obtain information about employees and applicants. The Federal Trade Commission (the “FTC”), which enforces the FCRA, indicated in an opinion letter that this definition includes agencies retained by employers to investigate employees with respect to workers' compensation claims and other private entities and organizations hired by employers to investigate workplace misconduct such as sexual harassment allegations, fraud and employee violence. This expansive definition has not been confirmed in any court, as it is uncertain whether the FTC's broad interpretation will be adopted.

A **creditor** is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Where non-profit and government entities accept deferred payment for goods or services, they, too, are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the National Credit Union Administration (NCUA), come under the jurisdiction of the Federal Trade Commission (FTC).

A **covered account is:** (i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes that involves or is designed to permit multiple payments or transactions such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

A **financial institution** is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that, directly or indirectly, holds a “transaction account” belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC’s jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

Identifying Information includes all of the items listed below (N.C.G.S. § 14-113.20(b)).

1. SSNs or employer identification numbers (EINs).
2. Drivers license, state identification card, or passport numbers.
3. Checking and savings account numbers.
4. Credit and debit card numbers.
5. Personal Identification Number (PIN) code, as defined in N.C.G.S. § 14-113.8(6).
6. Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names.
7. Digital signatures.
8. Any other numbers or information that can be used to access a person’s financial resources.
9. Biometric data.
10. Fingerprints.
11. Passwords.
12. Parent's legal surname prior to marriage.

Identity Theft is a fraud committed or attempted using the identifying information of another person without authority. (16 CFR 603.2(a))

Issue means to send out; put into circulation; or deliver for use.

A **notice of address discrepancy** is a notice sent to a user of a consumer report by a consumer reporting agency pursuant to 15 U.S.C. 1681c(h)(1), that informs the user of a substantial difference between the

address for the consumer provided by the user in requesting the consumer report and the address or addresses the consumer reporting agency has in the consumer's file.

A **person** is any individual, partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.

A **Red Flag** is a pattern, practice, or specific activity that indicates the possible existence of identity theft.

A **service provider** is a person that provides a service directly to the financial institution, creditor, or debit/credit card issuer that deals with covered accounts.

A **transaction account** is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

DHHS shall develop and implement an Identity Theft Prevention Program. As part of its program, divisions and offices shall assess whether they operate as a financial institution, a creditor that offers or maintains covered accounts and/or a debit/credit card issuer. If the division or office operates as either of these three, it is subject to this policy and must develop and implement the following procedure(s):

Financial Institution or a Creditor That Owns or Maintains Covered Accounts:

If the division or office determines that it operates as a financial institution or a creditor that owns or maintains covered accounts, the division or office must develop and implement reasonable procedures to detect, prevent and mitigate identity theft as part of the department's *Identity Theft Prevention Program*.

Debit/Credit Card Issuer:

If the division or office determines that it issues any form of monetary benefit (MT), including, but not limited to debit, EBT, credit cards or vouchers, it must develop procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card. These procedures will be incorporated into the department's Identity Theft Prevention Program.

User of a Consumer Report:

If the division or office determines that it uses consumer reports as part of its business operations, it must develop procedures to respond to a notice of address discrepancy received from a consumer reporting agency. These procedures will be incorporated into the department's Identity Theft Prevention Program.

Department Responsibilities

The Red Flags Rule sets out how certain businesses and organizations must develop, implement, administer and oversee their Identity Theft Prevention Program. The Program must include four basic

elements, which together create a framework to address the threat of identity theft.

The purpose of the Identity Theft Prevention Program is to detect, prevent, and mitigate identity theft in connection with new or existing covered accounts. It must be appropriate to the **size, complexity, nature,** and **scope** of the department's activities.

Elements of the Program

First, the department's Program must include policies and procedures to identify the "red flags" of identity theft that a division or office may run across in the day-to-day operations of its business. For example, if a customer has to provide some form of identification to open an account, an ID that looks like it might be fake would be a "red flag" for a division or office.

Second, the Program must be designed to detect the red flags the division or office has identified. For example, if a division or office has identified fake IDs as a red flag, it must have procedures in place to detect possible fake, forged or altered identification.

Third, the Program must spell out appropriate actions the division or office will take when it detects red flags.

Fourth, because identity theft is an ever-changing threat, the division or office must address how it will re-evaluate its Program periodically to reflect new risks from this crime.

If a division or office issues MT or uses consumer reports, the Program will also include procedures to:

- **Assess** the validity of a change of address for a MT account if an individual requests an additional or replacement card for the same account shortly thereafter; and/or
- **Enable** the recipient of a credit report, after receiving a notice of address discrepancy, to form a reasonable belief that a consumer's address has changed and to provide the reasonably confirmed address to the consumer reporting agency from whom it received the notice of address discrepancy.

Administration of the Program

DHHS provides for the continued administration of the *Identity Theft Prevention Program* by ensuring divisions and offices perform the following:

- **Obtaining** approval of the initial written Program from either the Secretary of DHHS (Secretary) or his or her designee;
- **Reporting to the Secretary** on exceptions, risks, and Program effectiveness;
- **Detecting, logging,** and **resolving** identified Red Flag exceptions;
- **Training management** and **staff** to effectively implement the divisions' and offices' procedures;
- **Exercising** effective oversight of Service Providers and binding them to compliance via contract;
- **Considering** the guidelines in Appendix B and **including** those guidelines that are appropriate in its procedures; and

- **Periodically monitoring** the divisions' and offices' procedures for changes in scope--which could include new covered accounts or red flags--legislation, and effectiveness.

Oversight, Development, Implementation and Administration of the DHHS Identity Theft Program

The Secretary of DHHS shall be responsible for designating an employee at the level of senior management to oversee the DHHS Identity Theft Program and assigning specific responsibility for the Program's implementation within the department.

DIVISION OR OFFICE RESPONSIBILITIES

In order for a division or office to determine whether the Red Flag and Address Discrepancy Policy applies to its business operations, the division or office should perform a **risk assessment** (*See Appendix A*) by asking itself the following preliminary questions:

1. Is your division or office a creditor or financial institution?
2. If so, does your division or office offer or maintain covered accounts?
3. Does your division or office any form of MT?
4. Does your division or office order credit reports on consumers from a consumer reporting agency?
5. Is your division or office a service provider for another DHHS division or office that is subject to the Red Flag and/or Address Discrepancy Rules?
6. Is the service your division or office provides to the DHHS division or office covered by the Red Flag and/or Address Discrepancy Rules?

Those divisions and offices that are subject to the Red Flag and Address Discrepancy Rules will be required to perform the following functions as part of the DHHS Identity Theft Prevention Program:

- Identify their covered accounts;
- Identify their relevant red flags;
- Review/develop mechanisms to detect red flags;
- Review/develop mechanisms to prevent, mitigate, and respond to identity theft incidents;
- Add the Red Flag and Address Discrepancy Rules' requirements to their current identity theft compliance program activities;
- Ensure Service Providers' compliance with the Red Flag and Address Discrepancy Rules (covered accounts, transaction accounts, or debit/credit cards);
- Provide employee training; and
- Provide oversight of and review its procedures for effectiveness.

Guidelines for Formulating and Maintaining an Identity Theft Prevention Program:

Detecting Red Flags

When the division or office performs a risk assessment and determines that it is subject to Red Flag Rule compliance, the division's or office's procedures should, at a minimum, address the detection of Red

Flags in connection with the opening of covered accounts and with existing covered accounts, such as by:

- Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests, in the case of existing covered accounts.

The procedures should include relevant Red Flags from the following five categories, as appropriate (*See Appendix B for specific examples*):

- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;
- The presentation of suspicious documents;
- The presentation of suspicious personal identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to, a covered account; and
- Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the financial institution or creditor.

Preventing, Mitigating, and Responding to Identity Theft Incidents

The division's or office's procedures should provide for appropriate responses to the red flags it has detected that are commensurate with the degree of risk posed. In determining an appropriate response, the division or office should consider aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a client's account records held by the division or office or third party, or notice that a client has provided information related to a covered account held by the division or office to someone fraudulently claiming to represent the division or office or to a fraudulent website. Appropriate responses may include the following:

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

Monetary Transactions, including Debit/Credit/EBT Card Issuers and Vouchers

A division or office that issues any form of MT must establish and implement reasonable policies and procedures to assess the validity of a change of address if it:

- Receives notification of a change of address for a consumer's MT account; and
- Within a short period of time afterwards (during at least the first 30 days), the division or office receives a request for an additional or replacement card for the same account.

Under these circumstances, the division or office is not allowed to issue an additional or replacement card, until:

- The cardholder is notified of the request:
- At the cardholder's former address; or
- By any other means of communication the division or office and the cardholder have previously agreed to use; and
- The cardholder is provided a reasonable means of promptly reporting incorrect address changes.

Oversight of Service Providers

Third-party service providers and business partners that handle information in covered, transaction, or MT accounts are probably one of the biggest risks related to identity theft. It is important for divisions and offices to be aware of how important this component is to the department's overall Identity Theft Prevention Program.

Whenever a division or office engages a service provider *outside of DHHS* to perform an activity in connection with one or more covered, transaction, or debit/credit card accounts on its behalf, the division or office should take the necessary steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. The division or office should require the service provider, **by contract** to do the following:

- Develop procedures to detect relevant Red Flags that may arise in the performance of its activities;
- Take appropriate steps to prevent identity theft;
- Mitigate identity theft immediately once it occurs; and
- Report all Red Flag incidents to the division or office within a specified time.

For example: The Office of the Controller (OC) contracts with the Attorney General's Office to collect outstanding client debt on its behalf.

Whenever a division or office is a service provider that performs an activity for another division or office that is subject to the Red Flag and Address Discrepancy Rules, the service provider will also be required to develop policies and procedures.

For example: The Office of the Controller performs billing functions for Central Regional Psychiatric Hospital. As part of its billing functions, OC offers or maintains covered accounts on behalf of Central

Regional Hospital. OC and Central Regional Hospital will be required to develop written procedures as part of the department's Identity Theft Prevention Program.

Recording and Reporting Incidents

The Identity Theft and Security Breach Notification Policy requires that each DHHS division and office assign an Identity Theft Coordinator to investigate and report inappropriate disclosures of identifying information. This same Identity Theft Coordinator will also be responsible for recording, investigating and reporting incidents involving covered account red flags, address discrepancies and debit/credit card accounts.

Each division and office should implement a process for investigating, mitigating and reporting incidents timely. If an incident occurs, the Identity Theft Coordinator shall notify the DHHS Privacy Officer immediately and forward the results of the investigation to the DHHS Privacy Officer when the investigation has been completed.

The Identity Theft Coordinator shall also submit a list of his or her division's or office's incidents to the DHHS Privacy Officer no later than December 31st of each year, providing a brief description of the incident, the date the incident occurred, and the resolution of the incident.

Respond to the receipt of a notice of address discrepancy from a consumer reporting agency

A division or office that uses consumer reports must develop and implement reasonable policies and procedures designed to enable it to form a reasonable belief that a consumer report relates to the client about whom it has requested the report, when the division or office receives a notice of address discrepancy.

Reasonable policies and procedures may include:

- Comparing the information in a consumer report provided by the consumer reporting agency with information the division or office:
- Obtains and uses to verify the consumer's identity in accordance with the requirements of the Customer Information Program (CIP) rules implementing 31 U.S.C. 5318(l),
- Maintains in its own records, such as applications, change of address notifications, other customer account records, or retained CIP documentation; or
- Obtains from third-party sources; or
- Verifying the information in the consumer report provided by the consumer reporting agency with the client.

The division or office must also develop and implement policies and procedures to reasonably confirm the accuracy of a consumer address that will be furnished to the consumer reporting agency from whom it received a notice of address discrepancy, when the division or office:

- Can form a reasonable belief that the consumer report relates to the client about whom the division or office requested the report;
- Has a continuing relationship with the client; and

- Regularly and in the ordinary course of business, furnishes information to the consumer reporting agency that sent the notice of address discrepancy.

NOTE: *The notification requirement exists only if a division or office regularly supplies information to the consumer reporting agency, and the confirmed address can be included in the division's or office's next regularly scheduled delivery of information to that consumer reporting agency.*

Reasonably confirming that an address is accurate

The division or office may reasonably confirm that an address is accurate by:

- Verifying the address with the client about whom it has requested the report;
- Reviewing its own records to verify the address of the client;
- Verifying the address through third-party sources; or
- Using other reasonable means.

NOTE: *The Federal Trade Commission (FTC) is interpreting this requirement as only applying to notices of address discrepancies on consumer reports, also known as credit reports, issued by nationwide consumer reporting agencies ("CRAs"), as defined in Section 603(p) of the Fair Credit Reporting Act ("FCRA"). Today, the FTC staff has stated there are only three such nationwide CRAs: Experian, TransUnion and Equifax. Therefore, as a practical matter, notices of address discrepancy on consumer reports issued by the "big three" entities (directly or through intermediaries) are the reports that the FTC staff believes are currently subject to this rule.*

The FTC has stressed that the obligation to conduct address verification only applies to a user of the consumer report that has received a "notice of address discrepancy" from one of the three nationwide CRAs. In other words, in the FTC staff's view, users of consumer reports, such as nursing homes, assisted living facilities or other health care entities, that may use consumer reports for employment or admissions purposes, are only technically required to perform the address verification upon receiving such an express "notice of address discrepancy."

DHHS Red Flag and Address Discrepancy Policy

Per the Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 16 CFR Part 681, the Red Flag and Address Discrepancy Policy has been approved for implementation within the NC Department of Health and Human Services (DHHS).

APPENDIX A

DHHS Red Flag and Address Discrepancy Assessment Questionnaire

In order for a North Carolina (NC) Department of Health and Human Services (DHHS) division or office to determine whether the Red Flag Rule applies to its business operations and if Identity Theft Prevention Program procedures must be developed, the division or office must ask itself the following questions:

Question 1: Is your division or office a creditor or a financial institution?

If NO, Go to Question 3.

If YES, Go to Question 2.

Question 2: Does your division or office offer or maintain covered accounts?

If NO, Go to Question 3.

If YES, Develop procedures as part of DHHS Identity Theft Prevention Program. Go to Question 3.

Question 3: Does your division or office order credit reports on consumers from a Consumer Reporting Agency?

If NO, Go to Question 4.

If YES, Develop procedures on how you will determine if your client's address has changed, after receiving a notice of address discrepancy from the consumer reporting agency. Go to Question 4.

Question 4: Does your division or office issue debit or credit cards?

If NO, Go to Question 5.

If YES, Develop procedures on how you will assess the validity of a change of address if you receive notification of a change of address for a debit/credit card account and within a short period of time afterwards, you receive a request for an additional or replacement card for the same account. Go to Question 5.

Question 5: Is your division or office a service provider for a DHHS division or office that is subject to the Red Flag and Address Discrepancy Rules?



If NO,

If YES, Go to Question 6.

Question 7: Is the service your division or office provides to the DHHS division or office covered by the Red Flag and/or Address Discrepancy Rules?



If NO,

If YES, Develop the applicable procedures based upon the service provided to the DHHS division or office.

APPENDIX B

Red Flags

from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.
2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
3. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of Part 681.
4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
 - a. A recent and significant increase in the volume of inquiries;
 - b. An unusual number of recently established credit relationships;
 - c. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
6. The photograph or physical description on the identification document is not consistent with the appearance of the applicant or customer presenting the identification.
7. Other information on the identification document is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
8. Other information on the identification document is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is the same as the address provided on a fraudulent application; or
- b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

- a. The address on an application is fictitious, a mail drop, or prison; or
- b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by another person opening an account or another customer.

15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for new, additional, or replacement cards or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example:

- a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example

- a. Nonpayment when there is no history of late or missed payments;
- b. A material increase in the use of available credit;
- c. A material change in purchasing or spending patterns;
- d. A material change in electronic fund transfer patterns in connection with a deposit account;
- or
- e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

APPENDIX C

Situations that could alert a creditor that an identity theft incident may be in progress or has already occurred in a health care setting

1. A complaint or question from a patient based on the patient's receipt of:
 - a bill for another individual;
 - a bill for a product or service that the patient denies receiving;

- a bill from a health care provider that the patient never patronized; or
- an Explanation of Benefits or other notice for health services never received.

An unexpected bill or notice of benefits can be one way that a patient can learn that she has been a victim of medical identity theft. “Explanations of Benefits” (EOB) are potentially important tools for patients and providers. For example, hotline information to report possible fraudulent or suspicious activity can be included on an EOB.

2. Records showing medical treatment that is inconsistent with a physical examination or medical history as reported by the patient. In particular, records that show substantial discrepancies in age, race, and other physical descriptions may be evidence of medical identity theft. An incorrect blood type is evidence that the patient was a victim of medical identity theft.
3. A complaint or question from a patient about the receipt of a collection notice from a bill collector. A collection notice can be one way that a patient can learn that she has been a victim of medical identity theft.
4. A patient or insurance company report that coverage for legitimate hospital stays are being denied because insurance benefits have been depleted, or that a lifetime cap has been reached. Members of a family can be victimized by “looping”, where a thief uses one family member’s benefits and then turns to the next family member when the first victim’s benefits have run out.
5. A complaint or question from a patient about information added to a credit report by a health care provider or insurer. An entry in a credit report can be one way that a patient can learn that she has been a victim of medical identity theft.
6. A dispute of a bill by a patient who claims to be the victim of any type of identity theft. Although financial identity theft differs significantly from medical identity theft, a victim of financial identity theft may be more likely to also be a victim of medical identity theft. Victims of financial identity theft may have filed police reports about their case, and these need to be taken into account.
7. A patient who has an insurance number but never produces an insurance card or other physical documentation of insurance. A medical identity thief may succeed by obtaining the medical insurance number and other information about the victim. The absence of an actual insurance card is evidence suggesting that the person being treated may not be the actual insured. Note: This particular Red Flag has to be applied with caution because there are other reasons a patient may not have her insurance card.
8. A notice or inquiry from an insurance fraud investigator for a private insurance company or a law enforcement agency. Not all forms of medical identity theft are the result of an individual thief presenting for treatment. Fraudulent billing by a physician can result in false information in a health record that may affect the treatment of patients. In some cases, clerks, nurses and other hospital employees have exploited their legitimate access to health files to use patients’ identity and health information for medical identity theft.

Chapter 4: Identity Theft and Security Breach Notification

In an effort to reduce the risk of exposing its citizens to the possibility of identity theft and to an information security breach, the North Carolina (NC) General Assembly enacted the NC Identity Theft Protection Act which became effective on December 1, 2005.

The NC Identity Theft Protection Act is comprised of two (2) statutes, which articulate when “businesses” and state or local governments can collect social security numbers (SSNs) and other identifying information; what they must do if they possess such information; and what notification responsibilities exist if “personal” or “identifying” information is disclosed without valid authorization.

The purpose of the Identity Theft and Security Breach Notification Policy is two-fold:

- Protect SSNs and other identifying information that DHHS receives, collects, uses, stores, discloses and mails in compliance with North Carolina General Statutes (N.C.G.S.) § 132-1.10; and
- Outline procedures and protocols for responding to a security breach involving the unauthorized disclosure of unencrypted personal information, in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

This policy is guided by the following objectives:

- To increase DHHS workforce members’ awareness about the confidential nature of SSNs and other identifying information;
- To reduce the reliance upon SSNs for identification purposes;
- To increase emphasis on the secure use, collection, transmission and storage of SSNs and other identifying information;
- To provide a consistent Department of Health and Human Services (DHHS) policy regarding the collection, usage, storage, transmission, mailing and disclosure of SSNs and other identifying information;
- To increase the confidence of clients and workforce members that SSNs and other identifying information are maintained in a confidential manner; and
- To institute consistent procedures for determining when a security breach has occurred and whether notice is required.

DHHS is dedicated to ensuring that its agencies protect SSNs and other identifying information of its clients and workforce members. **All** DHHS agencies, therefore, must comply with the Identity Theft and Security Breach Notification policy and immediately report any breach of security or compromise of systems containing this type of data to its designated personnel.

DHHS agencies should request an individual’s identifying information only when required to do so by federal or state law, or at the very minimum, only as necessary to conduct their legitimate business operations. Where the purpose of the identifying information can be satisfied by another personal unique identifier, reduced to the last four digits of the SSN or removed entirely, all DHHS agencies are expected to do so.

DHHS agencies that maintain SSNs and other identifying information in paper form or electronic media shall adhere to the following procedures with regard to its collection, usage, storage, transmission, mailing and disclosure, in compliance with N.C.G.S. § 132-1.10. They shall also immediately report any breach of security or compromise of systems containing personal information to designated personnel in compliance with N.C.G.S. § 132-1.10(c1) and N.C.G.S. § 75-65.

DHHS divisions and offices shall not collect SSNs unless and until:

- The collection is authorized by law or imperative for the performance of the agency's duties and responsibilities as prescribed by law;
- The collection is relevant to the purpose for which it is collected;
- The need for the collection has been clearly documented;
- The SSNs have been segregated on a separate page so they are easy to redact when there is a valid public records request; and
- A statement of the purpose(s) for which the SSN is being collected and used is provided to the individual, upon their request, at the time of **or** prior to the actual collection of the SSN.

DHHS agencies shall not use SSNs for any purpose other than the purpose stated in this policy. Usage shall be for a legitimate business purpose, and a duty exists to safeguard this data and prevent unnecessary access thereto.

Before storing any SSNs, DHHS agencies:

- shall first evaluate and determine whether there is a legitimate business need to store SSNs before this data can be stored in DHHS system applications, locked filed cabinets, or other storage containers.
- should reduce the SSN to the last four (4) digits, whenever possible, or replace it with a random identification number. When storage of the entire SSN is necessary, DHHS agencies should implement appropriate safeguards to prevent the possibility of workforce member misuse.

DHHS agencies shall not require an individual to transmit a SSN over the Internet unless the connection is secure **or** the SSN has been encrypted; or require an individual to use a SSN to access an Internet web site unless a password, unique identification number or other authentication device is also required.

Agencies shall not:

- Intentionally print or imbed a SSN on any card required to access government services (i.e. Medicaid, food stamps, etc.);
- Print a SSN on any mailed materials, unless state or federal law requires it;
- If required, print a SSN (in whole or in part) on a postcard or other mailer not requiring an envelope;
- Make a SSN visible on an envelope; or
- Make a SSN visible without the envelope having been

DHHS agencies **may** disclose SSNs, other identifying information or documents containing SSNs or other identifying information only in the following instances:

- Disclose to another governmental entity or its agents, employees, or contractors if disclosure is necessary for the receiving entity to perform its duties and responsibilities.
- Disclose pursuant to a court order, warrant, or subpoena;
- Disclose for public health purposes, pursuant to and in compliance with Chapter 130A;
- Disclose documents where SSNs or other identifying information have been redacted;
- Disclose SSNs or other identifying information on *certified* vital records issued by the NC State Registrar or authorized officials, pursuant to N.C.G.S. § 130A-93(c);
- Disclose any identifying information, **other than SSNs**, on *uncertified* vital records; or
- Disclose SSNs or other identifying information in a recorded document in the official records of the NC Register of Deeds office or in the Courts.

DHHS agencies must take reasonable measures to protect SSNs, and personal information against unauthorized access to or use of the information in connection with or after its disposal.

The reasonable measures may include:

- The burning, pulverizing or shredding of papers containing SSNs or personal information so this information cannot be practicably read or reconstructed; or
- The destruction or erasure of electronic media and other non-paper media containing SSNs or personal information so the information cannot practicably be read or reconstructed.

DHHS agencies may, after due diligence, enter into a written contract with, and monitor compliance by, a third party engaged in the business of record destruction to destroy SSNs or personal information. Due diligence should ordinarily include one or more of the following:

- Obtaining information about the disposal business from several references or other reliable sources and requiring that the disposal business be certified by a recognized trade association or similar third party with a reputation for high standards of quality review;
- or
- Taking other appropriate measures to determine the competency and integrity of the disposal business.

NOTE: It is the department's preference that the record destruction company shred documents containing SSNs and other confidential information onsite at the DHHS agency's location.

Chapter 5: Notice of Privacy Practices

Individuals served by a DHHS HIPAA-covered agency must be informed of their privacy rights and the agency's responsibility to protect their protected health information. The NC DHHS, as a covered entity, is required to provide a Notice of Privacy Practices in accordance with the HIPAA Privacy Rule, 45 CFR Subtitle A, Subchapter C, Part 164.

DHHS shall develop a general departmental Notice of Privacy Practices. This general Notice shall be designed to inform individuals of the department's legal duties and privacy practices with respect to the protected health information (PHI) it collects from them in general. Given that the scope of DHHS HIPAA-covered entities' use and disclosure may vary significantly, agencies designated as covered health care providers, health plans, or health care clearinghouses shall be required to develop and provide their own individualized Notice of Privacy Practices. DHHS HIPAA-covered entities designated as internal business associates (IBA), however, will be allowed to use the general Notice of Privacy Practices, unless the DHHS Privacy Officer deems otherwise.

Both types of Notice of Privacy Practices shall outline the uses and disclosures of PHI the department/agency may make, and shall notify individuals of their rights and the department's/agency's legal duties with respect to protecting their PHI. DHHS HIPAA-covered entities shall only use and disclose PHI in a manner consistent with their Notice of Privacy Practices.

Upon request, an agency shall make its Notice of Privacy Practices available to any individual(s), whether or not the individual is an agency client. The agency shall provide such Notice in a manner consistent with all requirements specified within this policy.

- A. **Development of Notices:** All Notice of Privacy Practices must contain the requirements outlined in 45 CFR § 164.520. In order to assist in ensuring that agencies' customized Notices contain all of the required elements, agencies should rely on the Notice of Privacy Practices Checklist and applicable templates for guidance.

Notices of Privacy Practices developed by DHHS HIPAA-covered entities shall be written in plain and simple language that a client, employee, or personal representative can easily read and understand.

Notices shall be made available in languages understood by a substantial number of clients served by each agency. At a minimum, each agency shall ensure its Notice is available in English and Spanish. DHHS agencies can request Braille Notices from the Division of Services for the Blind for clients who request such a format. Notices shall contain the elements described in the *Notice of Privacy Practices Required Elements* section of this policy.

- B. **Notice Revisions:** DHHS agencies shall promptly revise their privacy Notice whenever there is a material change to their client's rights or the agency's uses, disclosures, legal duties, or other privacy practices described in the Notice. A revised Notice shall be available upon request on or after the effective date of the revision.

Except when required by law, an agency shall not implement a material change to any term of the Notice prior to the effective date of the Notice in which such change is reflected.

Prior versions of an agency's Notice shall be retained for a period of at least six (6) years from the date of the last Notice delivery, or retained according to the agency's retention and disposition schedule, whichever is more stringent.

- C. **Provision of the Notice:** DHHS HIPAA-covered entities shall provide a written copy of their Notice of Privacy Practices to any individual requesting a copy, regardless of whether or not the individual is an agency client.

DHHS agencies that operate an Employee Health Service shall provide a written copy of their Notice of Privacy Practices to each employee at their first treatment encounter after April 14, 2003.

When providing individuals a Notice of Privacy Practices as required in this policy, an agency may provide their Notice to an individual by electronic mail (hereafter referred to as "e-mail") with a return receipt requested, if the individual agrees to an electronic Notice and such agreement has not been withdrawn. If the agency knows that the e-mail transmission failed, a paper copy of the Notice shall be provided to the individual. When a Notice is provided electronically, it shall meet the applicable delivery time requirements specified in this policy.

Any agency that maintains a Web site that provides information to the public about the agency's services or benefits shall prominently post its Notice on the Web site and make the Notice available electronically from the Web site. The Notice on the Web site shall reflect the most recent version.

DHHS HIPAA-covered entities do not have to provide their Notice to "inmates". "Inmates" include inmates from the NC Department of Correction and clients committed through the criminal justice system to a psychiatric hospital.

- D. **Approval Process:** All Notices and revisions to Notices must be submitted to the DHHS Privacy Officer for final approval prior to public distribution. The DHHS Privacy Officer will obtain Attorney General Office approval for agency Notices and revisions to Notices when necessary. Also, the DHHS Privacy Officer is responsible for forwarding Employee Health Service Notices to the Division of Human Resources for approval.

- E. **Additional Privacy Notice Requirements (Health Care Plans):**

Provision of the Notice: A DHHS HIPAA-covered agency designated as a health plan (i.e., Division of Medical Assistance) shall provide its Notice of Privacy Practices on a timely basis to its named insured (hereafter referred to as the "recipient"). New health plan enrollees shall receive a Notice no later than the time of enrollment. New enrollee Notices may be distributed at the time an application is filed, prior to determination of eligibility.

Notice Revisions: Whenever a DHHS health plan Notice is *materially* revised from the previous Notice, the revised Notice must be provided to the recipients then covered by the health plan within 60 days of the revision. When a Notice contains translated language

other than English, changes in the Notice to correct or improve the translation **is not** considered a material change.

Other Notification: At least once every **three (3) years**, the health plan shall notify the recipients then covered by the plan of the availability of the Notice and how to obtain a copy. At a minimum, this notification shall be presented in both English and Spanish. This notification may be combined with other communications sent routinely to recipients (e.g., Medicaid cards).

F. Additional Privacy Notice Requirements (Health Care Providers That Have a Direct Treatment Relationship with Clients):

Posting of the Notice: DHHS agencies that are health care providers who have a direct treatment relationship (e.g., face to face) with their clients, and who have a physical site where health care is provided directly to individuals, shall post the Notice in a clear and prominent location where it is reasonable to expect individuals seeking service from the agency will be able to read the Notice. DHHS agencies that operate an Employee Health Service shall post their Notice in the area where employees come for treatment.

Provision of the Notice: Except in an emergency situation, these agencies shall provide the Notice to clients or their personal representatives no later than the date of the first treatment service delivery, including service delivered electronically or via telephone. In an emergency treatment situation, the Notice shall be provided as soon as reasonably practicable.

If a covered health care provider's first treatment of an individual is delivered electronically, the agency shall automatically forward an electronic Notice to the individual. The individual who receives the electronic Notice retains the right to receive a paper copy upon request. If the first treatment encounter with the individual is by telephone, the Notice must be mailed within one working day of the telephone encounter. Scheduling an appointment is not considered a treatment encounter.

DHHS covered health care providers that provide residential services shall ensure that all clients in its residence as of April 14, 2003, are provided a Notice no later than April 14, 2003. Provision of the Notice can be met by having the client or personal representative read and return the Notice; however, the agency must provide the client or personal representative with a copy of the Notice upon request.

DHHS covered health care providers that are required to comply with federal regulation 42 CFR Part 2, relative to substance abuse, must provide their Notice of Privacy Practices to their substance abuse clients at the time of each admission. Otherwise, DHHS covered health care providers that have a direct treatment relationship with their clients need to provide the Notice initially and when revisions are made as noted below in the *Revision of Notice* section.

Acknowledgement of Receipt of the Notice: DHHS covered health care providers with a direct treatment relationship shall make a good faith effort to obtain a written

acknowledgment of receipt of the Notice from the client or personal representative, except in an emergency situation. If the first treatment encounter with the client is by telephone, mailing the Notice to the client and asking the client to return the signed acknowledgment in person or by mail shall be considered a good faith effort. When a Notice is delivered electronically, an electronic return receipt is considered a valid written acknowledgment of the Notice.

Should a client or personal representative be unable to sign his/her name on the acknowledgment, an "x" or other mark/symbol is acceptable in place of a signature, as long as it is witnessed and documented, attesting to the validity of the signature.

The Notice should provide a section for an acknowledgment. The agency shall keep the signed page as documentation of the receipt of Notice.

The DHHS covered health care provider shall not refuse to treat a patient because he/she would not sign a written acknowledgment; instead, it should document the good faith effort to obtain the signature. Documentation of a good faith effort shall include the date the Notice and acknowledgment was given/mailed to the individual, how it was delivered (in person, mailed, etc.), and the reason the acknowledgment was not signed (such as, patient refused or did not mail acknowledgment back to the covered health care provider).

Each provider agency shall establish a tracking process to ensure that each client was asked to sign the acknowledgment and that the signed acknowledgment was retained or a good faith effort documented.

The acknowledgment or good faith effort shall be filed in the client's medical record and retained in accordance with the agency's retention and disposition schedule for medical records, which shall be no less than six (6) years.

Revision of Notice: Whenever a DHHS health care provider's Notice is *materially* revised from the previous Notice, the revised Notice shall be available to clients or personal representatives upon request on or after the effective date of the revision. If a written acknowledgment was previously obtained or a good faith effort documented, another written acknowledgment is not required when the Notice is revised. In addition, the revised Notice must be promptly posted in a clear and prominent location where it is reasonable to expect individuals seeking service from the covered health care provider will be able to read the Notice. If the provider agency has a public Web site, the revised Notice shall be available on the Web site.

G. **Notice of Privacy Practices Required Elements:**

This statement shall be at the top of the Notice in a box: **"THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY."**

The Notice shall contain a description of the types of uses and disclosures that the HIPAA-covered agency is permitted to make for treatment, payment, and health care operations. At least one (1) pertinent agency example shall also be included.

A description of all other purposes for which the agency is permitted or required to use or disclose protected health information without the individual's written authorization.

If a use or disclosure for any purpose is prohibited or significantly limited by another applicable law, the description of such use or disclosure shall reflect the more stringent law.

For each purpose described, the description shall include sufficient detail to inform the individual of the uses and disclosures that are permitted or required by federal regulations as well as state and federal law.

A statement that other uses and disclosures will be made only with the individual's written authorization and that the individual may revoke such an authorization.

A statement that the covered entity is not permitted to use genetic information for underwriting purposes.

A statement regarding the covered entity's obligations to maintain the privacy of an individual's PHI and of the individual's right to receive notification, in the event of a breach involving their PHI.

In the event that the agency is a provider, the individual has the right to restrict disclosure of their PHI to a health plan, if the individual paid the provider, in full, for services rendered.

If the agency intends to engage in any of the following activities, the activity description shall include a separate statement accordingly:

- The agency may contact the individual to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the individual; or
- The agency may contact the individual to raise funds for the agency. An individual has the right to opt out of receiving such communications.

The Notice shall contain a statement of the individual's rights with respect to protected health information and a brief description of how the individual may exercise these rights, as follows:

- The right to request restrictions on certain uses and disclosures of protected health information, including a statement that the agency is not required to agree to a requested restriction;
- The right to receive communications of protected health information confidentially, as applicable;
- The right to inspect and copy protected health information;
- The right to request amendment to protected health information;

- The right to receive an accounting of applicable disclosures of protected health information; and
- The right of an individual, including an individual who has agreed to receive the Notice electronically, to obtain a paper copy of the Notice from the agency upon request.

The Notice shall contain the agency's duties, as follows:

- A statement that the agency is required by law to maintain the privacy of protected health information and to provide individuals with Notice of its legal duties and privacy practices with respect to protected health information, and to notify affected individuals following a breach of unsecured protected health information;
- A statement that the agency is required to abide by the terms of the Notice currently in effect; and
- A statement that the agency reserves the right to change the terms of its Notice and to make the new Notice provisions effective for all protected health information that it maintains prior to issuing a revised Notice.
- The statement shall also describe how it will provide individuals with a revised Notice.

The Notice shall contain:

- a statement that individuals may complain to the agency and to the Secretary of the United States Department of Health and Human Services if they believe their privacy rights have been violated.
- A brief description of how the individual may file a complaint with the agency and a statement that the individual will not be retaliated against for filing a complaint shall also be included in the Notice.
- The Notice shall contain the name or title, and telephone number of a person or office to contact for further information.
- The Notice shall contain the date on which the Notice is first in effect, which shall not be earlier than the date on which the Notice is printed or published.
- Certain uses and disclosures of PHI will require an authorization, such as psychotherapy notes, disclosure of PHI for marketing and disclosures that constitute a sale of PHI.

Chapter 6: HIPAA Violation Sanctions

The North Carolina Department of Health and Human Services (NC DHHS) has adopted a Sanctions policy in order to comply with our duties under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). HIPAA requires that covered entities have and apply appropriate sanctions against members of their workforce who fail to comply with the requirements of the Rule (45 CFR SS 164.530(e)(1)).

Any employee, volunteer, intern or business associate of the DHHS who works for a division/office that is a covered entity or a hybrid entity, under the definition of HIPAA, must review and sign the Department's HIPAA Sanctions Policy. DHHS shall impose appropriate measures, including disciplinary measures on any workforce member who violates this policy. Sanctions will be determined on a case by case basis, consistent with DHHS policies and procedures on disciplinary actions.

DHHS will investigate any violations of his policy and will impose disciplinary measures, up to and including dismissal on any workforce member who violates this policy. Violations and any subsequent disciplinary action shall be documented and reported to the appropriate human resources (HR) manager, the entity's Privacy Officer and a copy of such documentation shall be maintained in the workforce member's personnel file in accordance with DHHS policies and procedures on disciplinary actions. Violations may also carry federal civil and/or criminal penalties, and state criminal penalties.

Sanctions will not be applied to disclosures by employees who are acting in the capacity of a whistleblower or who are victims of a crime, or where the totality of the circumstances do not warrant sanctions.

Chapter 7: Privacy Official

The HIPAA Privacy Rule requires the designation of personnel who are responsible for the implementation of privacy policies and procedures, as well as personnel who are responsible for receiving complaints and answering questions concerning privacy.

DHHS, as a hybrid entity, must designate a privacy officer who is responsible for the coordination and implementation of all privacy and confidentiality efforts within the department. In addition, DHHS has determined that the department agencies that are defined in the purpose section of this policy must each designate a privacy official to act as the primary point of contact for the privacy of health information that is used within or disclosed outside of that agency. The DHHS Privacy Officer and Agency Privacy Officials are responsible for the coordination and facilitation of compliance activities associated with departmental privacy policies.

Responsibilities of the Department Privacy Officer:

The DHHS Privacy Officer shall oversee all activities related to the development, maintenance and adherence to department policies regarding the use and disclosure of individually identifiable health information, in accordance with state and federal laws as well as best business practices.

The responsibilities of the DHHS Privacy Officer shall also include, but are not limited to, the following:

- Act as the Department expert for issues related to privacy in the use and disclosure of health information.
- Serve as liaison with the North Carolina Office of the Attorney General in the analysis and application of state and federal privacy laws.
- Develop and maintain Department privacy policies related to the use and disclosure of health information.
- Provide guidance in the implementation of health information privacy policies and procedures.
- Provide consultation and direction regarding privacy and confidentiality of health information to agencies within the Department.
- Coordinate privacy activities within the department.
- Create educational awareness programs and ensure staff and extended workforce training is conducted.
- Monitor state and federal privacy legislation.
- Monitor DHHS compliance with DHHS privacy policies and report compliance level to management.
- Escalate privacy issues to DHHS management as appropriate.
- Communicate all Department expectations for privacy to Agency Privacy Officials.

The individual Agency Privacy Officials shall guide all agency activities related to adherence to DHHS privacy policies regarding the use and disclosure of individually identifiable health information, in

accordance with state and federal laws, best business practices, and under the direction of the DHHS Privacy Officer.

Agency Privacy Official responsibilities shall also include, but are not limited to, the following:

- Serve as primary agency contact for privacy issues and concerns regarding the use and disclosure of health information and for client rights regarding health information.
- Serve as the agency liaison to the DHHS Privacy Officer for privacy-related activities.
- Coordinate and facilitate efforts to support the agency in the accomplishment of their privacy compliance activities.
- If the DHHS agency is also a covered health care component under the HIPAA Privacy Rule (i.e., not an internal business associate), the Agency Privacy Official shall be responsible for responding to client requests for further information concerning the Notices of Privacy Practices.

DHHS agencies are responsible for ensuring agency compliance with department privacy policies. The following are some of the agency requirements in which the Agency Privacy Official may participate:

- Develop procedures based on department privacy policies to ensure the protection of individually identifiable health information within the agency.
- Implement agency privacy requirements by incorporating new privacy practices into existing business operations.
- Ensure applicable privacy training delivery to agency staff and extended workforce.
- Provide a designated agency contact for privacy complaints and ensure that all complaints are appropriately documented.
- Monitor agency compliance with DHHS privacy policies.
- Ensure appropriate use and disclosure of individually identifiable health information and client rights in regards to health information.
- Provide reasonable privacy protections for individually identifiable health information within the agency.

The DHHS Privacy Officer is designated by the Secretary of the DHHS. The DHHS Privacy Officer shall maintain the list of all agency privacy officials within the department.

Each agency defined in the purpose section of this policy shall designate a staff member to serve as the agency privacy official. These designees may have other primary job functions in addition to privacy responsibilities. The privacy officer will work closely with the HIPAA Coordinator when there is an incident investigation or breach involving HIPAA data.

Organizationally, privacy officials report to their supervisor within the agency. Agency privacy officials shall have an indirect reporting relationship to the DHHS Privacy Officer for privacy-related activities only. Upon request from the agency supervisor, the DHHS Privacy Officer shall provide input into the agency privacy official's annual performance evaluation as applicable to privacy-related activities.

Chapter 9: Workforce

Agencies shall ensure that members of their workforce and extended workforce make reasonable efforts to protect individually identifiable health information from intentional or unintentional use or disclosure that is in violation of the department's privacy policies and/or agencies' procedures. In the event that an agency should become aware of a privacy policy violation, the agency must make reasonable efforts to lessen any resulting harmful effects. Each agency shall ensure the protection of individually identifiable health information in a manner consistent with all requirements specified within this policy.

This policy covers students, volunteers, trainees, contractors, personnel working through a temporary agency, and other persons whose conduct in the performance of work for an agency is under the direct control of the agency, whether or not they are paid by the agency, who are hereinafter referred to as "extended workforce".

The HIPAA Privacy Rule addresses the protection of individually identifiable health information and mandates that covered entities provide appropriate privacy training to their workforce and extended workforce on the agency's policies and procedures regarding protected health information.

DHHS has determined that every agency in the department that maintains individually identifiable health information must comply with this workforce policy to ensure that members of the DHHS workforce and extended workforce understand the importance of privacy protections and the consequences of inappropriate uses or disclosures of individually identifiable health information.

Each agency shall ensure that its workforce and extended workforce are trained with respect to the protection of individually identifiable health information in accordance with the DHHS Privacy Policies and agency procedures, as appropriate in the performance of their job responsibilities. Training shall be provided to workforce/extended workforce with direct, inadvertent, or incidental access to such health information. This training is required for current members of the workforce and extended workforce, as well as new members of the workforce/extended workforce within a reasonable time after their employment. HIPAA training is available to all employees on the LMS system, and must be completed on a yearly basis.

Each agency shall develop procedures that ensure the appropriate privacy training of members of their workforce and extended workforce. Privacy training must be customized and categorized according to the level of access to individually identifiable health information required to fulfill job responsibilities. Basic privacy training must include awareness of the vulnerabilities of the health information in each agency's possession and procedures that must be followed to ensure the protection of that information as necessary for each individual to carry out his/her required job functions, including possible consequences for violation of privacy policies or procedures. Basic training is sufficient for some categories of staff, such as those staff members who are subject to inadvertent or incidental exposure to individually identifiable health information.

Each agency's procedures shall also provide for the documentation and retention of training attendance. Documentation of training shall include the workforce/extended workforce member's name, job title, date of training and type of training provided (e.g., basic privacy, comprehensive privacy). Training

attendance documentation shall be retained for no less than six (6) years from the last date of the individual's active participation as a member of the workforce or extended workforce. When contractor staff are working as members of the extended workforce (i.e., directly controlled by the agency verses a business associate relationship) and are working under a departmental contract, the department contract administrator shall retain the training documentation for those contractors.

When a change is made to DHHS Privacy Policies or agency procedures, each workforce member whose function(s) are impacted by the change shall receive the instruction necessary to implement the change within a reasonable amount of time after the change becomes effective.

All current agency workforce/extended workforce members with direct, inadvertent, or incidental access to individually identifiable health information shall be required to sign a Confidentiality Agreement acknowledging their understanding of the agency's privacy policies and procedures and the consequences of any violation.

All new workforce/extended workforce members with direct, inadvertent, or incidental access to individually identifiable health information shall be required to sign a Confidentiality Agreement within a reasonable amount of time after employment, but no later than upon completion of privacy training.

Confidentiality Agreements shall be retained for at least as long as the individual remains a member of the workforce or extended workforce.

Sanctions against employees who fail to comply with the DHHS privacy policies and/or agency procedures shall be in accordance with the State Personnel Act and related personnel policies, except that the sanctions for educators subject to Chapter 115C of the North Carolina General Statutes (NCGS) shall be in accordance with NCGS 115C-325. Appropriate sanctions for non-compliant contractors and other workforce members who are not state employees shall be imposed consistent with the terms of their contracts or operative working arrangements.

Agencies must review each incident individually, taking into consideration the severity of the incident, circumstances surrounding the incident, the harm done to the client and to the agency, and any possible repercussions as a result of the use or disclosure made by staff. All instances of sanctioning shall be documented through existing personnel processes.

The DHHS Privacy Officer and Agency Privacy Official, if one is designated in the agency, shall be notified of any privacy violations and, to the extent permitted by law, any sanctions applied.

DHHS agencies shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the following reasons:

- exercising his/her privacy rights;
- participating in any process relating to privacy compliance;
- filing a complaint with the Secretary of the U.S. Department of Health and Human Services;
- participating in a privacy related investigation, privacy compliance review, proceeding, or hearing; or

- engaging in reasonable opposition to any act or practice that the person believes to be unlawful as long as the action does not involve disclosure of individually identifiable health information.

Retaliation shall not occur for individuals who make a disclosure to a health oversight agency, public health authority, or an attorney retained by or on behalf of the individual to determine legal options, provided that the individual believes in good faith that an agency has done any of the following:

- performed an unlawful act;
- violated professional or clinical standards; or
- endangered a client or the public through the care, services, or conditions provided.

An agency is not considered to have violated HIPAA Privacy Rules if a member of its workforce or extended workforce who is the victim of a criminal act discloses individually identifiable health information to a law enforcement officer about the suspected perpetrator and the health information is the minimum needed to appropriately address the criminal act.

All business practices shall provide for preventing intentional unauthorized disclosure of individually identifiable information to unauthorized parties through written or oral interactions, as well as minimizing unintentional conveyance. Business practices shall also provide for reasonable efforts to lessen any resulting harmful effects in the event that an agency should become aware of a HIPAA Privacy Rule violation by the agency or an agency's business associate.

HIPAA covered agencies, DHHS Internal HIPAA Business Associates, and any DHHS agency that performs oversight or other services for a DHHS HIPAA covered entity shall require agency workforce and extended workforce to wear some form of visible identification when performing job responsibilities for that agency. An agency that promotes a residential environment for their clients may be excluded from staff identification at the discretion of the appropriate agency management.

Each agency must determine a reasonable method of employee identification. The method need not be costly. When workforce or extended workforce members conduct business in person that is likely to include the sharing of an individual's health information, the workforce/extended workforce member shall prominently display official agency identification that contains the member's name.

Chapter 9: Business Associates

DHHS workgroups that must comply with the HIPAA Privacy Rule are referred to as “covered health care components”. The HIPAA Privacy Rule requires covered health care components to identify persons or entities that provide specific functions, activities, or services that involve the use, creation, or disclosure of individually identifiable health information for, or on their behalf. Such entities are referred to as business associates.

It should be noted that the Omnibus Final Rule has expanded the definition of a business associate to include:

- Any downstream subcontractor that creates, maintains, receives or transmits PHI on behalf of a business associate, even if they have an indirect relationship with the covered entity;
- Health information organizations, e-prescribing gateways, or other persons that provide data transmission services to a covered entity that require routine access to PHI; and
- Any person that offers a personal health record to individuals on behalf of a covered entity.

Because the department had been determined to be a hybrid entity, each DHHS division and office was required to identify components that are covered by this HIPAA requirement. Although some components were determined not to be covered health care components under HIPAA, they do perform functions, activities, or services that involve the sharing of individually identifiable health information for, or on behalf of, covered health care components thus creating business associate relationships within this department. Such persons or entities **within** DHHS are health care components that are referred to as “**internal business associates**”.

Components in other NC state government departments/agencies or external contractors **outside** of DHHS that perform functions, activities, or services for, or on behalf of, a DHHS covered health care component, and involve the use, creation, or disclosure of individually identifiable health information are referred to as “**external business associates**”.

Functions, activities, and services performed by business associates that involve the use, creation, or disclosure of individually identifiable health information may include claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and re-pricing.

DHHS covered health care components are required to identify their **internal** business associates by recognizing all of the other divisions/offices (or portions thereof) within the department that perform specific functions, activities, or services for, or on behalf of, the covered component when such functions or activities involve the sharing of individually identifiable health information.

DHHS **internal** business associates must also identify their internal business associates by recognizing any other health care component(s) within DHHS that perform such functions, activities, or services for, or on behalf of, the internal business associate that involves the sharing of individually identifiable health information.

DHHS covered health care components and internal business associates must identify their **external** business associates by recognizing other NC state government departments/agencies and external

contractors (public and private) that perform specific functions, activities, or services for, or on behalf of, the covered component or the internal business associate when such functions, activities, or services involve the sharing of individually identifiable health information.

Business associates, as well as their subcontractors who have access to PHI, are now directly liable for failure to comply with the HIPAA Privacy and Security Rules. If they fail to do so, they can be assessed civil and criminal penalties.

Incidental access to individually identifiable health information while performing duties that do not typically involve the use or disclosure of such information generally does not constitute a business associate relationship.

Business Associate Agreements

DHHS covered health care components and internal business associates must initiate agreements with their external business associates in order to share individually identifiable health information while performing specific functions, activities, or services for, or on behalf of, the covered health care component or the internal business associate.

It is the responsibility of covered health care components and internal business associates to execute agreements with external business associates that provide satisfactory assurance that the business associate will appropriately safeguard individually identifiable health information.

A Business Associate is responsible for entering into Business Associate Agreements with its subcontractors. In turn, a subcontractor is responsible for entering into Business Associate Agreements with any of its own subcontractors “down the chain” of information flow.

Business Associate Agreements must be revised using the new DHHS standard BAA form, per the timeline stipulated by the OCR.

This revised Business Associate Agreement template, developed by the NC Office of the Attorney General, is required when contracts are initiated by DHHS staff. Such addenda must be attached to the department’s standard contracting template as specified in the DHHS Purchasing and Contracts Manual.

Certain external contractors may be considered part of the HIPAA covered component’s **workforce**, and therefore will not require a business associate agreement if the following criteria apply:

The workstation of the person under contract is on the covered health care component’s premises and

The person performs a substantial proportion of his/her activities at this location.

Any external contractor who is considered part of the covered health care component’s workforce must comply with that component’s privacy policies and procedures.

BAA are not required with contract agreements between agencies within DHHS since the DHHS Privacy Policy Manual applies to all DHHS agencies.

Disclosure of individually identifiable health information from one health care provider to another for treatment, consultation, or referral does not require a business associate agreement. (Note: For MH/DD/SAS agencies, a business associate agreement would not be required, but those agencies would have to initiate either a “service provider agreement”, according to NC General Statutes, or would have to secure client authorization to disclose health information to a health care provider outside the agency.)

A business associate agreement is also not required when individually identifiable health information is disclosed to a health plan for payment purposes.

DHHS covered health care components and internal business associates are required to take reasonable steps to correct any known material breach or violation of any business associate agreement. If such steps are unsuccessful, the agreement must be terminated, if feasible; and if not, the problem must be reported to the DHHS Privacy Officer who will determine if further actions are warranted, which could include reporting the problem and correction attempts to the United States Department of Health and Human Services.

Should a covered health care component or internal business associate become a business associate of an agency external to DHHS, the Standard DHHS BAA must be utilized. Under no circumstances should any changes be made to this agreement without the express agreement of the Attorney General’s office. If specific terms need to be addressed, they should be addressed in the contract, not the Business Associate Agreement.

Identifying Internal and External Business Associates

Each agency that has at least one covered health care component or internal business associate must evaluate specific functions, activities, and services that are provided for, or on behalf of, that component/business associate to identify all internal and external business associates as follows:

- Within the same DHHS division/office;
- Within other divisions in DHHS;
- Within other departments/agencies in NC state government; and
- Outside state government (external contractors).

Each agency must develop a process that identifies internal business associate relationships with other programs/units within the same division or with another division within DHHS. Components must maintain documentation of its internal business associates and update such information as internal business associates are added or deleted.

Each agency must also develop a process that identifies external business associate relationships at the time the agency initially creates a contract with the external contractor. Renewal of a contract that has a Business Associate Addendum requires a review of the Business Associate Agreement as well, for renewal purposes.

Covered components must identify all business associate relationships to standard contracts when entering contract information into the DHHS purchase and contracts database that monitors contracts.

The Workgroup for Electronic Data Interchange (WEDI) has created a **HIPAA/HITECH Business Associate Decision Tree** to assist in making this determination.

Contractual Documentation Requirements

There are no Business Associate Agreement contractual documentation requirements for services provided by internal business associates, other than the agency's general documentation requirements.

Documentation of services provided by external contractors is accomplished through a DHHS standard contract. Documentation of business associate requirements is accomplished in an addendum to the contract. Business Associate agreements must be maintained for at least ten(10) years from the date of creation.

Only contract templates created by the NC Attorney General's Office should be used for business associates agreements. These documents include all of the updated HIPAA requirements to which their contractors must agree before covered health care components are allowed to share individually identifiable health information.

Beginning July 18, 2013, all new or amended DHHS contracts must be evaluated to determine whether a business associate relationship exists. If a business associate relationship does exist, a Business Associate Agreement must be in place. For HIPAA compliant BAAs executed prior to the publication of the Final Rule (1/25/13), the executed BAA may remain in effect until 9/22/2014, or such time as it needs to be revised, whichever comes first. If a new BAA needs to be created, it must be executed prior to September 23, 2013.

Termination of Business Associate Relationship

Should a DHHS covered health care component or internal business associate become aware of a pattern of activity, or practice of an internal business associate that constitutes a material breach or violation of the internal business associate's obligation with respect to privacy of individually identifiable health information in its possession, such information shall be forwarded to the DHHS Privacy Officer for resolution.

Should a DHHS covered health care component or internal business associate become aware of a pattern of activity or practice of an external business associate that constitutes a material breach or violation of the external business associate's obligations with respect to individually identifiable health information specified in a contract or other arrangement, reasonable steps should be taken to cure each breach, end the violation, and/or mitigate the consequences.

If such steps are unsuccessful, the covered health care component or internal business associate may, at its discretion:

- Terminate the contract or arrangement, if feasible; or If termination is not feasible, the agency privacy official is responsible for reporting the breach to the DHHS Privacy Officer. The DHHS Privacy Officer is responsible for resolution, which may include reporting the problem to the US DHHS Secretary at:

Office for Civil Rights
U.S. Department of Health & Human Services
Atlanta Federal Center, Suite 3B70
61 Forsyth Street, S.W.
Atlanta, Georgia 30303-8909
Phone: (404) 562-7886

Tracking of Business Associates

Each agency is required to track their internal business associates by maintaining current documentation of their internal business associates throughout the year.

DHHS agencies shall track their external business associates through the contracts that are entered into the department database for purchasing and contracts.

Training

DHHS covered health care components and internal business associates are not required to provide privacy training to their external business associates; nor are they required to monitor the privacy protections for individually identifiable health information that are instituted by their external business associates.

Please note that there is a Department approved Business Associate Agreement template. It has been created by the Office of the Attorney General and there is to be no deviation from this form.

Chapter 10: Legal Occurrences

There are situations where Health Care organizations are required to use and/or disclose individually identifiable health information to an outside source. Client authorization is not required for these uses and disclosures. These situations shall be identified in this policy as “legal occurrences.” This includes disclosing individually identifiable health information when responding to judicial and administrative proceedings, court orders (including protective orders), subpoenas, law enforcement, and other legal mandates.

North Carolina (NC) law requires that certain individuals receive confidential information or records, upon demand; however, there may be federal laws that supersede the state requirements such as the federal Substance Abuse Regulations. The HIPAA requires agencies to verify the identity and authority of individuals requesting individually identifying health information prior to releasing such information to them. Examples of individuals and groups who may need individually identifiable health information include:

- The chief medical examiner or a county medical examiner who is investigating the death of a DHHS client;
- The director of social services or designee who is investigating a case of known or suspected child abuse or neglect;
- The guardian ad litem representing a child in a case of known or suspected child abuse or neglect;
- A guardian ad litem representing a minor between the ages of 14 and 16 who wants to marry;
- The NC State Child Fatality Prevention Team/ the NC Child Fatality Task Force/ a community or local child protection and review team that are involved in the review of a child’s death;
- The NC Secretary of DHHS when it has been determined that there is a “clear danger to public health;” and
- The state or local health director when pertaining to the diagnosis, treatment, or prevention of communicable disease.

NC law also requires that individually identifiable health information be released in the following circumstances:

- Known or suspected child abuse or neglect, child dependency, and child deaths believed to be due to maltreatment;
- Belief that a disabled adult is in need of protective services;
- Known or suspected cases or outbreaks of communicable diseases;
- Wounds and injuries caused by firearms;
- Illnesses caused by poisoning;
- Wounds or injuries caused by knives or other sharp instruments and a physician suspects a criminal act;
- Any other wound, injury, or illness wherein a treating physician suspects criminal violence was involved;
- Client-specific information for the central cancer registry; and

- Symptoms, diseases, conditions, trends in the utilization of health care services, or other health-related information that the State Health Director determines is needed to conduct a public health investigation of a possible terrorist incident.

DHHS agencies shall use or disclose individually identifiable health information as “required by law” wherein a federal, state, tribal, or local law compels an agency to make a use or disclosure of confidential information and that is enforceable in a court of law such as:

- Court orders;
- Court ordered warrants;
- Subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information;
- A civil or authorized investigative demand;
- Medicare conditions of participation with respect to health care providers participating in the program; and
- Statutes or regulations that require the production of information (including those that require such information if payment is sought under a government program providing public benefits).

All uses and disclosures of confidential information that are required by law must comply with and be limited to the requirements of the applicable law.

Each DHHS agency shall review other state and federal laws with which the agency must comply to determine if any provision of state law is contrary to a requirement of the HIPAA Privacy Rule. Such review is entitled “preemption analysis” and shall be conducted on a provision-by-provision basis of each state and federal law. If a state law relating to the privacy of individually identifiable health information is more stringent than a privacy regulation, state law shall not be preempted, thus providing greater privacy protections for a client.

As a rule, DHHS agencies shall not disclose individually identifiable health information without first obtaining written authorization from the client who is the subject of the request or the client’s personal representative, unless there is a court order that requires disclosure of confidential information. This rule applies when responding to:

- Requests presented by way of judicial or administrative proceedings.
- Subpoenas;
- Law enforcement officials (apart from when reporting a crime on the premises such as ‘escapees’ or ‘missing children’); or
- Warrants.

Any administrative investigator or prosecutor, including investigators of Medicaid fraud that are not expressly authorized by federal or state law, must present a court order before an agency may disclose individually identifiable health information.

There are various legal occurrences when DHHS agencies may disclose individually identifiable health information without authorization. These instances include:

- Responding to court orders (including protective orders);
- Requests specifically authorized by state or federal law (as may be the case for certain health oversight activities, auditing, licensing, and disciplinary actions); or
- Responding to law enforcement officials when reporting a crime, so long as federal or state requirements do not forbid or limit the disclosure.

Each DHHS agency shall identify all of the state and federal laws and regulations that apply to that agency's components and shall review the requirements for using and disclosing individually identifiable health information. Agencies shall determine which law/regulation is more stringent and provides the most protections for the confidential information maintained on the agency's clients such as laws that:

- Prohibit or restrict a use or disclosure when the privacy regulation would permit it;
- Provide clients with greater rights of access or amendment to their health information;
- Require covered health care components to provide clients with more information about uses, disclosures, rights, and remedies;
- Require express legal permission from a client that is more limiting in scope or reduces the effect of the permission;
- Require covered health care components to retain or report information for the accounting of disclosures that is more detailed or is for a longer duration; or
- Provide greater privacy protection for the client.

Preemption analysis may be limited to those provisions in laws and regulations that apply to the use and disclosure of individually identifiable health information maintained by HIPAA covered health care components.

There may be instances where a client may be involved in a legal proceeding, either conducted by a court of law or a government agency. In such proceedings attorneys, judges and others involved with the proceeding may contact a DHHS agency to access a client's individually identifiable health information.

Subpoenas

When DHHS agencies receive a subpoena for individually identifiable health information, it must be determined whether the subpoena resulted from a judicial or administrative order. If a court or administrative tribunal issues the subpoena, confidential information may be disclosed without authorization. A subpoena received from any other entity must be accompanied by an **authorization** from the client whose individually identifiable health information is being requested or a **court order** to release such information.

Court Order

An order issued by a judge that specifically identifies the individually identifying health information to be disclosed. Agencies must comply with court orders.

Involuntary Commitment

Agencies may disclose individually identifiable health information without authorization. Such disclosure is permitted by both state law and the HIPAA Privacy Rule when initiating the involuntary commitment process of an individual.

Incompetency Hearing

Disclosure of individually identifiable health information without authorization is permitted by both state law and the HIPAA Privacy Rule when initiating incompetency status.

Commitment Hearings and Rehearings

Agencies must provide certified copies of written results of examinations by physicians and records in cases of clients voluntarily admitted or involuntarily committed to the client's counsel, the attorney representing the state's interest, and the court in district or superior court hearings. Individually identifiable health information shall be preserved in all matters except those pertaining to the necessity for admission or for continued stay in a DHHS facility or commitment under review. The relevance of health information for which disclosure is sought shall be determined by the court with jurisdiction over the matter

Forensic Clients – Court Ordered Exam

Agencies may send the results or the report of a client's mental examination to the clerk of court, to the district attorney or prosecuting officer, and to the attorney for the defendant when a mental examination has been ordered by the court.

Reporting Child Abuse or Neglect

Agencies are required to report child abuse and neglect. When reporting child abuse or neglect cases, demographic data and information relative to the suspected abuse or neglect may be reported without authorization to the DHHS Department of Social Services.

(NOTE: The federal substance abuse regulations exception allowing programs to comply with mandatory child abuse reporting requirements under state law applies only to the initial reports of child abuse or neglect, and to a written confirmation of that initial report. All other reporting requires authorization from the client or the client's personal representative.)

Reporting Adult Abuse or Neglect

Agencies are required to report adult abuse and neglect, unless prohibited by federal law.

(NOTE: The federal substance abuse regulations do not address adult abuse or neglect.) When reporting adult abuse or neglect cases, demographic data and information relative to the suspected abuse or neglect may be reported without authorization.

Reporting Communicable Disease/Injuries/Danger

Agencies are required to report communicable diseases, serious wounds, and injuries. A responsible professional in the agency may disclose confidential information without authorization from the client when in the professional's opinion there is an imminent danger to the health or safety of a client or another individual; or when there is likelihood of the commission of a felony or violent misdemeanor.

Reporting for Master Client Index

Mental Health, and Developmental Disabilities, and Substance Abuse Services (MH/DD/SAS) facilities may furnish client identifying information to DHHS for the purpose of maintaining an index of clients service in state MH/DD/SAS facilities.

Legal Disclosures

DHHS agencies may receive requests for individually identifiable health information that are legally allowed in specific situations, which are listed below.

Specialized Government Functions (i.e., Law Enforcement/Secret Service/FBI)

Agencies may disclose confidential information to agents representing specialized government functions as long as the request is reasonable, the identity of the requestor is verified, and there are no laws that prohibit such disclosure.

Provide only the following protected health information when assisting law enforcement officials for the purposes of identification and location:

- Name and address;
- Date and place of birth,
- Social Security Number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death (as applicable); and
- A description of distinguishing physical characteristics (e.g., height, weight, gender, race, hair and eye color, presence or absence of beard or mustache, scars, and tattoos)

Next of Kin

MH/DD/SAS residential facilities may disclose the fact of admission or discharge of a client to the client's next of kin whenever the responsible professional determines that the disclosure is in the best interest of the client; however, if the client is present or available and capable, the agency may not make such disclosure unless the client agrees, is provided an opportunity to object but expresses no objection, or the agency reasonably infers from the circumstances that the client does not object.

Internal Client Advocates (MH/DD/SAS)

An internal client advocate shall be granted, without authorization of a client or the client's personal

representative, access to routine reports and other confidential information needed to fulfill the advocate's monitoring and advocacy functions. In this role, the advocate may re-disclose such information to the facility director or other staff who are involved in the treatment of the client.

External Client Advocates (MH/DD/SAS)/Long Term Care Ombudsmen

External client advocates and Long Term Care Ombudsmen must obtain prior written authorization from a client or the client's personal representative before being granted access to that client's confidential information, unless other federal laws permit access. Access to information shall be limited to that which is specified in the authorization.

Accounting of Disclosures

Agencies are required to keep a record of any paper, electronic, or verbal disclosure of individually identifiable health information made in response to the legal occurrences as specified in this policy.

Chapter 11: Authorizations

DHHS agencies shall disclose individually identifying health information only upon authorization by the client (or personal representative), unless state or federal law allows for specific exceptions. Authorizations obtained or received for disclosure of individually identifiable health information must be consistent with authorization requirements identified in this policy. An authorization ***permits***, but does ***not require***, a DHHS agency to disclose individually identifiable health information.

All DHHS agencies shall utilize the standard authorization form, It is written in plain and simple language that a client or personal representative can easily read and understand. The standard authorization shall be made available in languages understood by a substantial number of clients served by each agency. At a minimum, the department shall ensure the standard authorization in Spanish translation is available to DHHS agencies. Braille authorization forms shall be available to clients who are blind from the DHHS Division of Services for the Blind, upon request for such format.

DHHS divisions and offices may add their agency's identification information and form number to the standard form; however, any other alterations to the standard form must be prior approved by the DHHS Privacy Officer, who is responsible for the development and maintenance of the DHHS standard authorization form. Each agency is responsible for printing its own authorization forms.

The DHHS standard authorization form shall contain the core elements listed below. Any authorization form received by a DHHS agency from an agency/individual outside of DHHS shall be honored only if it contains the following elements:

- A specific and meaningful description of the information to be used or disclosed;
- The name or other specific identification of the person or class of persons authorized to make the requested use or disclosure of the information;
- The name or other specific identification of the person or class of persons to whom the use or disclosure can be made;
- A description of each purpose of the requested disclosure (the statement "at the request of the client" is a sufficient description of the purpose when a client initiates the authorization and does not, or elects not to, provide a statement of the purpose);
- An expiration date or event that relates to the client or the purpose of the use or disclosure. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:
 - The statement "end of the research study" or similar language is sufficient if the authorization is for use or disclosure of individually identifying health information for research.
 - The statement "none" or similar language is sufficient if the authorization is for the agency to use or disclose individually identifying health information for the creation and maintenance of a research database or research repository; and
- Signature of the client and the date of the signature. If a client's personal representative signs the authorization form, a description of the personal representative's authority to act on behalf of the client must also be provided.

In addition to the required elements, the authorization form must contain statements that inform the client of the following:

- The client's right to revoke the authorization, the exceptions to the right to revoke, and a description of how the client may revoke the authorization;
- The consequences (as identified in the "Conditioning of Authorizations" section of this policy) to the client for refusal to sign the authorization form; and
- The potential for information to be subject to re disclosure by the recipient and no longer protected by state or federal law.

Each agency must provide a copy of the signed authorization to the client (or personal representative) upon request.

An authorization shall be considered invalid if the document has any of the following deficiencies:

- The expiration date has passed or the expiration event is known to have occurred;
- The authorization form is not completely filled out;
- The authorization form does not contain the core elements of a valid authorization;
- The authorization is known to have been revoked;
- Any information recorded on the authorization form is known to be false; or
- An authorization for psychotherapy notes is combined with a request for disclosure of information other than psychotherapy notes.

A separate authorization must be obtained for disclosure of the personal notes of a mental health professional that are separated from the rest of a client's record, except as follows:

- Use by the originator of the psychotherapy notes for treatment purposes;
- Use or disclosure by a DHHS agency for its own training programs in which students, trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family or individual counseling;
- Use or disclosure by the DHHS agency to defend itself in a legal action or other proceeding brought by a client;
- Investigations by the Secretary of the US Department of Health and Human Services;
- Use or disclosure required by law;
- Health oversight activities;
- Coroners and medical examiners; or
- Institution review board or Privacy Board approval for waiver of authorization for research purposes.

Questions regarding the agency's authority to disclose psychotherapy notes without a valid authorization should be referred to the DHHS Privacy Officer.

An authorization for disclosure of individually identifiable health information shall not be combined with any other written legal permission from the client (e.g., Consent for Treatment, Assignment of Benefits); however, research studies that include treatment may combine authorizations for the same research study, including consent to participate in the study.

An authorization for disclosure of psychotherapy notes may not be combined with any other authorization; however, psychotherapy notes that are needed from more than one provider or are disclosed to more than one recipient may be combined.

Agencies may use a single authorization for disclosure to multiple agencies involved in coordination of care.

An authorization that specifies a condition for the provision of treatment, payment, enrollment in a health plan or eligibility for benefits may not be combined with any other authorization.

The provision of treatment, payment, enrollment in a health plan or eligibility for benefits shall not be conditioned on whether or not a client signs an authorization form, except as follows:

- The provision of research-related treatment can be conditioned on a client authorizing the use or disclosure of individually identifiable health information for such research;
- Provision of health care solely for the purpose of creating individually identifiable health information for disclosure to a third party (e.g., physical exam for life insurance); or

Prior to enrollment in a health plan if authorization is for eligibility or enrollment determinations and the authorization is not for disclosure of psychotherapy notes.

Signatures

Each authorization must be signed and dated by the client (or personal representative). If a client's personal representative signs the authorization form, a description of such authority to act for the client must also be documented on the form.

In any of the mental health/developmental disabilities/substance abuse services institutions operated under the authority of DHHS, whenever the health information of a minor or incompetent adult is to be disclosed to an external client advocate, both the client and the personal representative must sign the authorization.

In the psychiatric hospitals and alcohol and drug abuse treatment centers operated under the authority of DHHS, when minors are receiving treatment for alcohol or substance abuse, based upon the consent of their personal representative, the minor and personal representative must both sign the authorization.

G.S. 90-21.5 allows a provider to treat a minor client without consent of a parent or personal representative. When the minor consents to treatment, only the minor is required to sign the authorization.

Should a client (or personal representative) be unable to sign his/her name, an "x" or other mark/symbol is acceptable in place of a signature, as long as it is witnessed and documented, attesting to the validity of the signature.

Dates

Each authorization must state an expiration date or event, such as a specific time (e.g., January 1, 2003); a specific time period (e.g., one (1) year from the date of signature); or an event directly relevant to the client or the purpose of the disclosure (e.g., 60 days following discharge from the facility). Unless revoked sooner by the client, an authorization will be valid for a period up to one (1) year, except for financial transactions, wherein the authorization shall be valid indefinitely.

The expiration date or event for each authorization must be acknowledged and actions taken on that authorization must be consistent with such limitations.

Revocation of Authorization

The authorization must state that a client has the right to revoke the authorization at any time, except to the extent that the DHHS agency has already taken action based upon the authorization. The department strongly recommends that clients be encouraged to sign a revocation statement that becomes a permanent part of the record. Should a client refuse to sign a request for revocation, the verbal revocation statement should be witnessed by a third-party and documentation of the request should be placed in the client's record. The authorization form must include instructions on how the client may revoke an authorization.

Retention Period

DHHS agencies that maintain authorization forms in their client records must adhere to the retention period in the agency's retention and disposition schedule for client records.

If authorization forms are maintained separately from client records, the authorization forms must be maintained in accordance with the *General Schedule for State Agency Records* issued by the North Carolina Department of Cultural Resources, Division of Archives and History, Archives and Records Section, Government Records Branch.

Photocopy/Facsimile Authorizations

An original authorization form is preferred for disclosure of individually identifiable health information; however, a clear and legible photocopy/facsimile is acceptable.

Contractor Authorizations

The authorization requirements contained in this policy also apply to contractors who perform a service for or on behalf of a DHHS agency. Such contractors are limited to those disclosures permitted in an agreement with the agency. Contractors are responsible for ensuring these policy requirements are enforced with any sub-contractors they may use.

Chapter 14: Consent for TPO

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule allows covered health care components to use individually identifiable health information within the facility and to disclose individually identifiable health information outside the facility without consent from the client or the client's personal representative for the purposes of treatment, payment, and health care operations. NC General Statute (GS) 122C-53(a) requires written consent for disclosure of confidential information unless there are other state laws that permit such disclosures without consent; therefore, NC law preempts the HIPAA Privacy Rule and consent must be obtained prior to release of individually identifying health information for specific treatment, payment, and health care operation purposes not otherwise allowed by law.

The DHHS Consent for TPO allows staff in each facility to share and use the health information of clients who are receiving treatment in their facility and to disclose individually identifiable health information outside the facility for treatment, payment, and health care operation purposes. This *consent* **does not** replace each facility's *Consent for Treatment*, nor does it replace the *DHHS Authorization to Disclose Health Information* for disclosing individually identifiable health information for purposes other than treatment, payment, or health care operations.

Facilities operated by DMH/DD/SAS shall obtain written consent from the client or personal representative prior to use and disclosure of individually identifiable health information for the purposes of treatment, payment, and health care operations. No covered health care component may condition treatment on the client providing consent for treatment, payment, and health care operations.

Without such consent, no individually identifiable health information may be disclosed outside the covered health care component unless there is an authorization from the client.

The signed *DHHS Consent for TPO* shall be considered valid for the period of time needed to fulfill its purpose for treatment and health care operations for up to one (1) year, after which time a new consent must be completed and signed. Any time during the year whenever a new person or agency not covered in the consent form is identified as a recipient of individually identifiable health information for TPO, a new *DHHS Consent for TPO* or an authorization from the client must be completed. For payment purposes, the consent is valid until the need for disclosure is satisfied.

The department shall provide a template for use by all facilities in developing their consent forms for using and/or disclosing individually identifiable health information for treatment, payment, or health care operations. The consent template shall contain the basic elements required by state and federal laws and regulations. Agencies may add additional elements to meet the needs of each facility.

Facility procedures must specify the differences in requirements and implementation of:

- DMH/DD/SAS Consent for TPO
- Facility Consent for Treatment
- DHHS Authorization to Disclose Health Information

Procedures

- Each facility shall develop their procedures for obtaining each client's consent for using individually identifiable health information within that covered health care component and for disclosing such information outside that covered health care component for the purposes of treatment, payment, or health care operations.
- Each facility shall develop an individualized consent form utilizing such elements as deemed necessary for that facility.
- Each facility shall make a "good faith effort" to obtain consent for treatment, payment, and health care operations upon admission of a client.

Exceptions to the consent requirement permit use and disclosure without consent as follows:

- Should a client's mental condition be such that it is impossible for the client to understand and sign a consent for TPO, such information must be documented
- Should a client be admitted in an emergency situation, such information must be documented and consent for TPO should be obtained when the client has stabilized.
- Should a client be involuntarily admitted and refuse to sign consent, such information must be documented and signature of the consent for TPO should be attempted at a later date.
- Should there be a substantial communication barrier and the client clearly does not understand the process, such information must be documented and consent for TPO should be obtained when a translator is available to explain the need for consent.
- Should a client understand the request and refuse to sign consent, such information must be documented including the attempt and the reason the client would not sign.

Each facility must develop and implement procedures for obtaining consent for treatment, payment, and health care operations from all new clients at the time of admission after the effective date of this policy. Facilities must also develop a policy and procedure for consent requirements when the same client is readmitted to the facility before the original consent expires. Procedures should include the process staff should follow when a client does not wish to consent to the use of or disclosure to all of the people/agencies listed on the consent template (e.g., allowing the client to strike through and initial the changes/deletions they desire.)

It is acceptable for facilities to phase-in the consent requirement for clients who were already residing in the facility on the implementation date of this policy. For long-term clients, it is recommended that such consent be obtained at the client's annual review, unless the need to disclose information comes before the annual review, at which time the consent would be obtained. Facilities must develop the agency's process for obtaining consent from long-term clients who were already residing in the facility prior to the implementation date of this policy and must determine if consent should be obtained at the time of their annual review or sooner.

Any time a disclosure for treatment, payment, or health care operations is to be made to a person or agency that is not covered on the consent form, facilities must initiate a new *DHHS Consent for TPO* or an authorization that identifies the new entity. Staff must be instructed that until the *DHHS Consent for TPO* is obtained from clients already residing in the facility, the facility may disclose information for treatment and health care operations only as identified in the agency's *Notice of Privacy Practices*.

Facilities must document and implement the agency's process for informing staff of these rules.

Chapter 15: USE AND DISCLOSURE

The final Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule controls the use and disclosure of individually identifiable health information. Generally, covered health care components may not use or disclose individually identifiable health information except in ways identified in the Privacy Rule or when required or allowed by other federal or state laws. All other uses are prohibited and barriers must be established to prevent any use and disclosure other than those permitted. 'Use' and 'disclosure' are significant terms that distinguish sharing of information within an agency (use) from releasing information outside an agency (disclosure).

DHHS agencies may not use or disclose individually identifiable health information except either:

- As this policy permits or requires or
- As the individual who is the subject of the information authorizes in writing

It should be understood that throughout this policy whenever a 'client' is addressed, the client's 'personal representative' (including a guardian) shall be treated the same as the client, when the client is unable to act for him/herself

HIPAA requires DHHS agencies to disclose individually identifiable health information in the following situations:

- To clients specifically when they request access to their health information (although there are exceptions that are identified in this policy), or when they request an accounting of disclosures of their health information and
- To the Secretary of the United States (US) Department of Health and Human Services (HHS) when undertaking a compliance investigation, review, or enforcement action.

Permitted Uses and Disclosures

HIPAA permits DHHS agencies to use and disclose individually identifiable health information without a client's written authorization for the following purposes or situations:

- To a client (except as required for access and accounting of disclosures);
- Treatment, payment and health care operations (exceptions for DPH and MH/DD/SAS agencies. Incidental to an otherwise permitted use and disclosure;
- Limited data set [for research, public health, or health care operations)
- Facility directories (unless a client opts out of the directory);
- Notification/involvement with family/others;
- Disaster relief;
- Required by law;
- Public Health activities;
- Abuse and neglect;

- Health oversight activities;
- Judicial and administrative proceedings ;
- Law enforcement purposes;
- To avert serious threat to health/safety;
- Specialized government functions;
- Workers' Compensation; and
- Research with Institutional Review Board (IRB) approval (see DHHS Privacy Policy Use and Disclosure Policies, Research).

Agencies must rely on professional ethics and best judgment when deciding which of these permissive uses and disclosures to make.

DHHS agencies may use and disclose individually identifiable health information only with a client's authorization for the following purposes or situations:

- To anyone, for any reason, that is not for treatment, payment, or health care operations; or otherwise permitted or required by state or federal law/regulation;
- If the individually identifiable health information to be used or disclosed is psychotherapy notes; and

DHHS agencies must make reasonable efforts to use, disclose, and request only the minimum amount of individually identifiable health information needed to accomplish the intended purpose of the use, disclosure, or request for information, except for the following circumstances:

- Disclosure to or a request by a health care provider for treatment purposes;
- Disclosure to a client who is the subject of the information;
- Use or disclosure made pursuant to an authorization;
- Disclosure to HHS for complaint investigation, compliance review, or enforcement;
- Use or disclosure that is required by law; or
- Use or disclosure required for compliance with other HIPAA rules

Clients may request agencies to restrict all or a portion of their individually identifiable health information from specific uses or disclosures. DHHS agencies that have agreed to such restrictions are required to use and disclose the restricted information only as agreed.

DHHS agencies that have created information that is not individually identifiable do not have to comply with the use and disclosure requirements, provided that:

- Disclosure of a code or other means of de-identification that can be used to re-identify the client, constitutes disclosure of individually identifiable health information; and

- If de-identified health information is re-identified, DHHS agencies must use or disclose such re-identified information only in accordance with the use and disclosure requirements in this policy Disclosures to Business Associates

DHHS agencies may disclose individually identifiable health information of clients to a business associate and may allow a business associate to create or receive a client's individually identifiable health information on its behalf [see DHHS Privacy Policy Administrative Policies, Business Associates (Internal/External)].

DHHS agencies must use and disclose individually identifiable health information of a deceased client in the same manner as if the client were still alive. Under the HIPAA Omnibus rule, a decedent's PHI only need be protected for a period of fifty years.

DHHS agencies must use and disclose individually identifiable health information to a personal representative of a client in the same way as the agency would to the client, with two exceptions:

- If the client is an un-emancipated minors (under specific circumstances); and
- In abuse, neglect, and endangerment situations. Confidential Communications

DHHS agencies must make reasonable efforts to comply with requests from clients to disclose confidential communications by alternative means or methods

Disclosures by Whistleblowers and Workforce Member Crime Victims

DHHS agencies shall not be considered in violation of use and disclosure regulations if a member of its workforce or its business associate discloses individually identifiable health information "in good faith" to a health oversight agency or attorney retained by or on behalf of the individual; or if individually identifiable health information is disclosed to law enforcement by a workforce member who is a victim of crime, abuse, neglect, or domestic

Food and Drug Administration

DHHS agencies may use or disclose individually identifying health information to:

- Collect and report adverse events that are subject to the jurisdiction of the Food and Drug Administration (FDA) as related to the quality, safety, or effectiveness of such FDA-regulated products or activities;
- Enable product recalls, repairs, and replacements; and
- Conduct post-marketing surveillance.

Communicable Diseases

DHHS agencies shall disclose individually identifiable health information regarding a client(s) who has been exposed to a communicable disease or may otherwise be at risk of contracting or spreading a

disease or condition, according to requirements set forth in Chapter 130A of the NC General Statutes (GS).

DHHS agencies may disclose individually identifiable health information to an employer about a client who is a member of the employer's workforce if the employer has requested the agency conduct an evaluation relating to medical surveillance of the workplace or to evaluate the client for a work-related illness or injury. Information disclosed shall be limited to the work-related illness or injury of the client or to carry out its responsibilities for workplace medical surveillance

Client rights provided by the HIPAA Privacy Rule require agencies to disclose individually identifiable health information to the client who is the subject of the information, unless an agency has a compelling reason not to do so.

The HIPAA Privacy Rule requires agencies to disclose individually identifiable health information to the HHS Secretary, when requested, to determine compliance with the HIPAA Privacy Rule. Agencies are required to maintain proper records, and upon request of HHS, to submit compliance reports in such time and manner as determined by the HHS Secretary.

During an investigation or compliance review, DHHS agencies must cooperate with HHS and the DHHS Privacy Officer shall be notified of such investigation or compliance review.

- Agencies must permit access by HHS during normal business hours to its facilities, books, records, accounts, and other sources of information, including individually identifiable health information, that are pertinent to ascertaining compliance with the requirements or investigation of a complaint.
- If HHS determines that serious circumstances exist, agencies must permit access by HHS at any time and without notice.
- If any information required of DHHS agencies is in the exclusive possession of any other agency, institution, or person and the other agency, institution, or person fails or refuses to furnish the information, DHHS agencies must so certify and set forth what efforts it has made to obtain the information.

Variations in requirements specific to disclosure to the Secretary of US HHS include the following:

- Written authorization from the client is not required for such disclosures.
- Disclosures to HHS are not subject to the minimum necessary requirements.
- Disclosures to HHS are required to be accounted for in the agency's Accounting of Disclosures log.

DHHS agencies shall use and disclose individually identifiable health information without client authorization only as permitted or required in this policy, or as required by other federal or state laws and regulations. **Whenever North Carolina General Statutes and other federal regulations are more stringent than the HIPAA privacy rules, the more stringent requirement prevails.**

Although client authorization is not required by law or regulation in the following circumstances, each agency should exercise professional judgment in determining whether to seek client involvement when using or disclosing that client's confidential information.

Treatment Purposes

Individually identifiable health information may be **used** (i.e., shared among designated staff) within a covered health care component to carry out treatment activities. DHHS agencies may use a client's individually identifiable health information for its own treatment purposes, including coordination and management of health care services for clients.

- Use of individually identifiable health information by the workforce within an agency for treatment purposes does not require written authorization from the client.
- Use of individually identifiable health information by the workforce for treatment purposes is not subject to the minimum necessary requirements.
- Use of individually identifiable health information by the workforce for treatment purposes is not required to be accounted for in the agency's Accounting of Disclosures log.
- Use of psychotherapy notes requires a written authorization from the client who is the subject of the notes.

One Client/One Record – Facilities within the Division of Mental Health, Developmental Disabilities and Substance Abuse Services (DMH/DD/SAS) shall share one client record for all treatment services rendered to each individual client within all Division facilities to coordinate treatment, payment, etc. The agency's Consent for TPO allows the client record to be "used for treatment purposes" within all of the Division facilities. (The DMH/DD/SAS Client Records Manual for State Facilities, APSM 45-3 should be consulted in determining the procedures for sharing one health record per client.)

Corporate Master Person Index: Facilities within Division of Mental Health, Developmental Disabilities, and Substance Abuse Services are required to furnish individually identifiable health information to the Department for the purpose of maintaining a database of clients served in the state facilities. State facilities may access this database only if such information is necessary for the appropriate and effective evaluation, care, and treatment of a client.

Individually identifiable health information may be **disclosed** (e.g., shared with other health care providers or human service agencies) outside a covered health care component to carry out treatment coordination and management between providers and for referrals to other health care providers for treatment purposes.

- Disclosure of individually identifiable health information by the workforce in an agency for treatment purposes does not require written authorization from the client.

- Disclosures of individually identifiable health information by the workforce in an agency to another health care provider for treatment purposes are not subject to the minimum necessary requirements.
- Disclosures of individually identifiable health information for treatment purposes are not required to be accounted for in the agency's Accounting of Disclosures log.

Payment Purposes

Individually identifiable health information may be **used** (i.e., shared among designated staff) within a covered health care component for payment purposes such as determining or fulfilling the agency's responsibility for coverage and provision of benefits under a health plan; or to obtain or provide reimbursement for the provision of health care.

- Use of individually identifiable health information by the workforce within an agency for payment purposes does not require written consent from a client.
- Use of individually identifiable health information by the workforce within an agency for payment purposes is subject to the minimum necessary requirement.
- Use of individually identifiable health information by the workforce within an agency for payment purposes is not required to be accounted for in the agency's Accounting of Disclosures log.

Individually identifiable health information may be **disclosed** (e.g., shared with other payers, health care providers, or business associates) outside a covered health care component to carry out payment functions such as eligibility, billing, claims adjustment, and other collection activities.

- Disclosure of individually identifiable health information by the workforce outside the agency for payment purposes does not require written authorization from the client.
- Disclosure of individually identifiable health information by the workforce in an agency for payment purposes are subject to the minimum necessary requirements.
- Disclosure of individually identifiable health information by the workforce in an agency for payment purposes are not required to be accounted for in the agency's Accounting of Disclosures log.

Health Care Operations

Individually identifiable health information may be **used** (i.e., shared among designated staff) within a covered health care component for health care operation purposes such as conducting quality assessment and improvement activities, business planning and development, business management and administrative activities, student training, and credentialing.

- Use of individually identifiable health information by the workforce within an agency for health care operation purposes does not require written consent from the client.

- Use of individually identifiable health information by the workforce for health care operation purposes is subject to the minimum necessary requirements.
- Use of individually identifiable health information by the workforce for health care operation purposes is not required to be accounted for in the agency's Accounting of Disclosures log.

Individually identifiable health information may be **disclosed** (i.e., shared with entities) outside a covered health care component to carry out health care operation functions such as accreditation, licensure, conducting or arranging for medical review, auditing, or legal services that are necessary to run the agency and to support the core functions of health care treatment and payment.

- Disclosure of individually identifiable health information by the workforce in an agency for health care operation purposes does not require written authorization from the client.
- Disclosure of individually identifiable health information by the workforce in an agency for health care operation purposes is subject to the minimum necessary requirements.
- Disclosure of individually identifiable health information for health care operation purposes is not required to be accounted for in the agency's Accounting of Disclosures log.

DHHS agencies may use or disclose individually identifiable health information in certain circumstances, but agencies must allow clients the opportunity to agree, object, or restrict certain uses or disclosures of their individually identifiable health information, in advance of the agency's use or disclosure. Such information must be documented in the client's health record.

- Written authorization from a client is not required for such disclosure.
- Oral agreement or objection by a client is acceptable.
- Disclosures for which a client must have an opportunity to agree or object are subject to the minimum necessary requirements.
- Disclosures for which a client must have an opportunity to agree or object are not required to be accounted for in the agency's Accounting of Disclosures log.

The following circumstances require agencies to provide clients with the opportunity to agree or object to the use or disclosure of their individually identifiable health information:

- Facility directory/emergency situations;
- Notification or involvement of family member, other relative, or close personal friend of a client in the client's care or payment related to the client's health care; and
- Disaster relief purposes.

1. Facility Directory/Emergency Situations

DHHS facilities may use the following individually identifiable health information to maintain a directory of facility clients:

- Client name;
- Client location in facility;
- Client condition (in general terms such as good, fair, poor); and
- Client's religious affiliation.

Notification/Involvement with Family/Others

In situations where individually identifiable health information of a client is being disclosed to a family member, other relative, or close personal friend of the client **and the client is present**, the agency must obtain the client's agreement, provide the client with an opportunity to agree or object to the disclosure, or determine, based on the circumstances and using professional judgment, that the client would not object prior to the disclosure. **If the client is not present** or is incapacitated and cannot agree or object, the agency must use professional judgment to determine what is in the best interest of the client. In such instances, agencies must limit the information being disclosed to that which is directly relevant to the situation.

NOTE: Chapter 122C of the NC General Statutes define specific circumstances and conditions when confidential information can be disclosed to family/others by MH/DD/SAS facilities. These facilities shall develop procedures consistent with NC state law.

Disaster Relief

Use or disclosure of individually identifiable health information for disaster relief purposes (e.g., flood, hurricane, terrorism) must be determined based on professional judgment, taking into account the best interest of the client, and the determination that the requirements do not interfere with the ability to respond to the emergency circumstances.

DHHS agencies may use or disclose individually identifiable health information without written authorization and without an opportunity for the client to agree, object, or restrict certain uses or disclosures of their individually identifiable health information in specific circumstances.

Required by Law

DHHS agencies may use and disclose individually identifiable health information to the extent that such use or disclosure is required by law, and the use or disclosure complies with and is limited to the relevant requirements of such law. Legal mandates requiring use or disclosure of individually identifying health information may be based upon federal or state statutes/regulations, board of health rules, court orders, and subpoenas issued by a court or other similar judicial or administrative body.

Examples of uses or disclosures required by law include the following:

- The Chief Medical Examiner or a county medical examiner may demand the records of a patient who has died and whose death is under investigation (NCGS 130A-385).
- Local health directors or the State Health Director may demand medical records pertaining to the diagnosis, treatment, or prevention of communicable disease (NCGS 130A-144(b)).

- If a health care provider reports an event that may indicate an illness, condition, or health hazard caused by terrorism to a local health director or the State Health Director, the State Health Director or local health director may demand to see records that pertain to those reports (NCGS 130A-476).
- Physicians must report known or suspected cases or outbreaks of reportable communicable diseases to the local health department (NCGS 130A-135)/
- Physicians, local health departments, and DHHS shall, upon request and without consent, release immunization information to schools (public, private, or religious), licensed and registered childcare facilities, Head Start, colleges and universities, health maintenance organizations, and other state and local health departments outside North Carolina [NCGS 130A and 10A NC Administrative Code (AC) 41A].
- Health care providers and administrators of health care facilities must report the following types of wounds/injuries to law enforcement authorities: wounds and injuries caused by firearms; illnesses caused by poisoning; wounds and injuries caused by knives or other sharp instruments if it appears to the treating physician that a criminal act was involved; any other wound, injury, or illness involving grave bodily harm if it appears to the treating physician that criminal violence was involved (NCGS 90-21.20).
- All health care facilities and health care providers must report diagnoses of cancer to the central cancer registry (NCGS 130A-209).
- State statutes require all live births, fetal deaths, and deaths, including required medical information related to births and medical certification of the cause of death, to be reported to the local registrar in the county where the birth or death occurred. Physicians, hospitals, medical facilities, birthing facilities, funeral directors, medical examiners, and others as specified are required to provide this information (NCGS 130A-90 - 130A-123).

NOTE: Reports made to newspapers or other media regarding birth and/or death announcements require authorization.

Procedural requirements for disclosures required by law include the following:

- Written authorization from the client is not required for such disclosures; however, if authorization is obtained, verbal request and authorization is sufficient.
- Disclosures required by law are subject to the minimum necessary requirements unless the law specifies otherwise.
- Disclosures required by law are required to be accounted for in the agency's Accounting of Disclosures logs.

Public Health Activities

There are specific laws that **require** information related to public health activities to be disclosed so those laws would fall under the "required by law" provisions noted in the corresponding section above.

There are also some laws that **permit** information related to public health activities to be used or disclosed. DHHS agencies may disclose individually identifiable health information related to public health activities to a public health authority when such uses or disclosures are permitted under the law for:

- Prevention and control of disease, injury, and disability;
- Communicable disease notification;
- Child abuse and neglect reporting;
- FDA-regulated product or activity monitoring; and
- Work-related illness or injury monitoring and workplace medical surveillance.

Public health authorities may include the following organizations and individuals:

- Federal: Components and officials of HHS including those within the Centers for Disease Control and Prevention (CDC) and the FDA. The American Association of Poison Control Centers is acting under a cooperative agreement with the CDC to conduct the toxic exposure surveillance system, thus is functioning as a public health authority.
- State: Components and officials of NC DHHS (Division of Public Health), the NC Department of Environment and Natural Resources (DENR), and the NC Department of Agriculture, as well as parallel agencies in other states.
- Local: Components and officials of local health departments and boards of health. Other non-traditional public health authorities might include a county sheriff's office or a private, non-profit organization that is responsible for animal control activities such as rabies control. For child abuse and neglect reporting, the county departments of social services.
- Other: An organization performing public health functions under a grant of authority from or contract with a public health agency [45 Code of Federal Regulations (CFR) 164.501] such as universities, community-based organizations, and others, who in these situations are considered public health authorities when performing public health activities.

In addition to public health authorities, DHHS agencies may also disclose individually identifiable health information to an official of a foreign government agency that is acting in collaboration with a public health authority if the public health authority directs the agency to make such disclosure.

For example, if the CDC is collaborating with public health officials in Canada while investigating a disease outbreak, a NC DHHS agency could disclose protected health information to a Canadian government agency if directed to do so by the CDC.

Examples of uses or disclosures permitted for public health purposes for the “prevention and control of disease, injury, and disability; and communicable disease notification” include the following:

- Health care providers are permitted to report any event that may indicate an illness, condition, or health hazard caused by terrorism to local health directors or the State Health Director (NCGS 130A-476).
- Medical facilities are permitted to report certain communicable diseases to the local health director (NCGS 130A-137).
- Hospitals and urgent care centers are permitted to participate in a program for reporting emergency department data to a program established by the State Health Director for public health surveillance purposes (NCGS 130A-476).
- The State Center for Health Statistics is permitted to collect health data for various health-related research purposes on a voluntary basis – they cannot compel mandatory reporting (NCGS 130A-373).

Child Abuse and Neglect Reporting

Under North Carolina law, any person or institution who has cause to suspect that any juvenile is abused, neglected, or dependent, or has died as the result of maltreatment must make a report to the department of social services in the county where the child lives or is found (NCGS 7B-301).

FDA-regulated Product or Activity Monitoring

Agencies must disclose individually identifiable health information to the FDA when required to do so as related to the quality, safety, or effectiveness of such FDA-regulated products or activities. Agencies must ensure staff are aware of such requirements and shall develop a process for ensuring the reporting is handled according to agency requirements. Staff must be knowledgeable of such requirement and assured that the disclosure is not in violation of the agency’s privacy policies and procedures.

Work-Related Illness or Injury Monitoring and Workplace Medical Surveillance

DHHS physicians, medical facilities, and laboratories are required to report to the Department all cases of specified serious and preventable occupational injuries that occur while working on a farm, as well as specified serious and preventable occupational diseases and illnesses which result from exposure to a health hazard in the workplace. DHHS agencies shall ensure procedures are in place to report required injuries, diseases, and illnesses.

DHHS agencies shall develop procedures regarding disclosures for “public health activities that may be made to an employer” about an individual who is a member of the employer’s workforce or an individual who is receiving health care at the request of the employer in the following circumstances:

- To conduct an evaluation relating to medical surveillance of the workplace or
- To evaluate whether the individual has a work-related illness or injury.

The individually identifiable health information disclosed must directly relate to the above circumstances. DHHS agencies must provide the individual with a written notice that such information is disclosed to an employer, for public health activity purposes.

Procedural requirements for disclosures for “public health activities” include the following:

- Written authorization from the client is not required.
- Disclosures are subject to the minimum necessary requirements, unless the law specifies otherwise.
- Disclosures are required to be accounted for in the agency’s Accounting of Disclosures log.

Adult Abuse and/or Neglect Reporting

Under North Carolina law (Article 6, Chapter 108A), any person having reasonable cause to believe that a disabled adult is in need of protective services must make a report to the director of social services.

In making such disclosure, agency staff shall promptly inform the client, in the exercise of professional judgment, that such a report has been or will be made, except if a qualified professional believes informing the client would place the client at risk of serious harm; or if it is determined by agency staff that informing a client’s personal representative would not be in the best interest of the client.

Procedural requirements for disclosure when reporting “adult abuse and/or neglect” include the following:

- Written authorization from the client is not required.
- Individually identifiable health information disclosed for such purposes is not subject to the minimum necessary requirements, but professional judgment should be exercised in determining the information that is necessary to meet the purpose.
- Such disclosures are required to be accounted for in the agency’s Accounting of Disclosures log.

Health Oversight Activities

DHHS agencies may disclose individually identifiable health information to a health oversight agency for health oversight activities authorized by law, including audits, investigations, inspections, licensure, or disciplinary actions, legal proceedings or actions, or other activities necessary for appropriate oversight of:

- The health care system;
- Eligibility programs;
- Compliance with program standards; or

- Compliance with civil rights laws.
Exception: Investigation or other activity in which the client is the subject of the investigation or activity that is not directly related to the client's health care, claim for benefits or receipt of public services is not considered a health oversight activity. Procedural requirements for disclosures related to "health oversight activities" include the following:
 - Written authorization from the client is not required.
 - Disclosures are not subject to the minimum necessary requirements.
 - Disclosures are required to be accounted for in the agency's Accounting of Disclosures log unless the health oversight activity is considered a health care operation. Health care operations may include accreditation, certification, peer review, licensing, or credentialing activities; conducting or arranging for medical reviews (e.g., death reviews); legal services; auditing functions, including fraud and abuse detection and compliance programs; and resolution of internal grievances.

Judicial and Administrative Proceedings

DHHS agencies may disclose individually identifiable health information for judicial or administrative proceedings, as required by NC General Statutes, when the use or disclosure is made in response to a(n):

- Court order;
- Administrative tribunal order;
- Subpoena;
- Discovery request; or
- Other lawful purpose.

All disclosures made in judicial and administrative proceedings shall be made only after the identity and authority of any person requesting such disclosure has been verified, and the requisite documentation required for the disclosure has been obtained. A subpoena alone is not sufficient reason for disclosing confidential information. Both a subpoena and a court order must be issued to compel disclosure.

Law Enforcement Purposes

DHHS agencies shall develop procedures that ensure staff is knowledgeable about disclosures that may be made for law enforcement purposes. Agencies may disclose individually identifiable health information without client authorization for the following law enforcement purposes as applicable:

- A law which requires disclosure such as reporting of wounds;
- Court order, court-ordered warrant, subpoena, or summons;
- Grand Jury subpoena;
- Administrative request including subpoena, summons, or civil or authorized demand; or
- Similar process authorized by law.

A subpoena alone is not sufficient reason for disclosing confidential information. Both a subpoena and a court order must be issued to compel disclosure.

Agencies may also disclose limited information for identification and location purposes when requested by a law enforcement official for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person. Only the following information may be disclosed:

- Name and address;
- Date and place of birth;
- Social Security Number;
- ABO blood type and Rh factor;
- Type of injury;
- Date and time of treatment;
- Date and time of death, if applicable; and
- A description of physical characteristics.

NOTE: There may be federal or state laws that are more restrictive than the requirements in this policy in which case the more restrictive would apply.

Procedural requirements for disclosures for “law enforcement purposes” detailed in this section include the following:

- Written authorization from the client is not required.
Exception: Individually identifiable health information related to DNA; dental records; or typing, samples, or analysis of body fluids or tissue **may not be disclosed without client authorization.**
- Disclosures are subject to the minimum necessary requirements, unless the law (including court orders) specifies otherwise.
- Disclosures are required to be accounted for in the agency’s Accounting of Disclosures log.

Victims of a Crime

DHHS agencies may disclose individually identifiable health information in response to a law enforcement official’s request for such information about a client who is, or is suspected to be, a victim of a crime if:

- The client agrees to the disclosure; or
- The agency is unable to obtain the client’s agreement because of incapacity or other emergency circumstances, provided that:
- A violation has occurred;
- Enforcement activity would be adversely affected if delayed; and
- Disclosure is in the best interest of the client.

Crime on Premises

DHHS agencies may disclose individually identifiable health information to a law enforcement official when the agency believes a crime (or threat of crime) has been committed on the premises or against agency staff. However, information disclosed must be limited to the circumstances and client status, including last known name and address.

Reporting Crime in Emergencies

If staff in a DHHS agency provides emergency health care in response to a medical emergency off site, the agency may disclose individually identifiable health information to law enforcement officials if such disclosure appears necessary to alert law enforcement to:

- The commission and nature of a crime;
- The location and the victim of such crime; and
- The identity, description, and perpetrator of such crime.

If the agency believes that the medical emergency off site is the result of abuse or neglect of the individual in need of emergency health care, the agency must first use professional judgment to determine if disclosure of individually identifiable health information is in the best interest of the individual.

Avert Serious Threat to Health or Safety

Agencies may use and disclose individually identifiable health information to avert a serious threat to health and safety whenever such use or disclosure is consistent with laws and ethical standards and the agency believes it is necessary to:

- Prevent or lessen a serious and imminent threat to the health or safety of a person or to the public, and the disclosure is to a person or entity that may reasonably be able to prevent or lessen the threat; or
- Assist law enforcement to identify or apprehend an individual;
- Where it appears from all the circumstances that the client has escaped from a correctional institution or from lawful custody; or
- Because of a statement by a client admitting participation in a violent crime that the agency reasonably believes may have caused serious physical harm to the victim.

NOTE: Disclosure is NOT permitted if the agency learned such information when treating, counseling, or providing therapy for such criminal conduct; or if the client requested to be referred for treatment, counseling, or therapy for such criminal conduct.

Information disclosed shall be limited to the client's statement and the following identifying information:

- Name and address;
- Date and place of birth;
- Social Security number;
- ABO blood type and Rh factor;
- Type of injury (if applicable);
- Date and time of treatment;
- Date and time of death (if applicable); and
- A description of distinguishing physical characteristics.

Unless otherwise prohibited by state or federal law, agencies may use or disclose individually identifiable health information for specialized government functions, as long as the identity of the individual representing such function is verified. Functions include:

- The Red Cross, Armed Forces personnel, or other authorized agents of the Armed Forces, if deemed necessary by appropriate military command;
- Authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities;
- Authorized federal officials for the provision of protecting the US President or foreign heads of state;
- Authorized federal officials for national security, which may include any of the agencies listed below.
 - The Office of the Director of the Central Intelligence Agency (CIA)
 - The Office of the Deputy Director of the CIA
 - The National Intelligence Council (and other such offices as the Director may designate)
 - The CIA
 - The National Security Agency
 - The Defense Intelligence Agency
 - The National Imagery and Mapping Agency
 - The National Reconnaissance Office
 - Other offices within the Department of Defense for the collection of specialized national intelligence through reconnaissance programs
 - The intelligence elements of the Army, Navy, Air Force, Marine Corps, Federal Bureau of Investigation, Department of the Treasury, and Department of Energy
 - The Bureau of Intelligence and Research of the Department of State
 - Other elements of any other department or agency as may be designated by the President, or designated jointly by the Director of Central Intelligence and the head of the department or agency concerned, as an element of the intelligence community

- The Department of State to make medical suitability determinations regarding required security clearance, mandatory service abroad, or for a family to accompany a Foreign Service member abroad;
- A correctional institution or law enforcement official with lawful custody of an inmate if necessary for the health and safety of such individual, other inmates, officers, or other employees at the correctional institution; and
- Government programs that provide public health benefits and governmental agencies administering such programs.

Procedural requirements for disclosures for “specialized government functions” include the following:

- Written authorization from the client is not required.
- Disclosures are subject to the minimum necessary requirements, unless the law specifies otherwise.
- Disclosures are required to be accounted for in the agency’s Accounting of Disclosures log.

Agencies may use or disclose individually identifiable health information as authorized by, and to the extent necessary to comply with laws relating to workers’ compensation or other similar programs established by law that provide benefits for work-related injuries or illness without regard to fault.

Personal Representative

A personal representative is any adult who has decision-making capacity and who is willing to act on behalf of a client regarding the use and disclosure of the client’s individually identifiable health information. This would include an individual who has authority, by law or by agreement from the client receiving treatment, to act in the place of the client such as spouse, adult children, parents, legal guardians, or properly appointed agents (e.g., an individual who has been given a medical power of attorney). Procedures must be developed that address when a personal representative is required and the responsibilities of the agency when communicating with a personal representative. Procedures must also include communication requirements if the client is an un-emancipated minor or if the client has been abused, neglected, or has been in an endangerment situation and there is some question about the personal representative’s involvement in the care of the client.

Client Photographs

Agencies that take photographs of clients for identification purposes must obtain the client’s consent prior to photographing. Photographs of clients may not be displayed in the facility or released outside of the agency without client authorization. Agencies may develop their own consent forms allowing the photograph(s) to be taken, but if there is a need to disclose the photograph(s), authorization must be obtained prior to disclosure.

Psychotherapy Notes

Psychotherapy notes are notations that capture a therapist’s impressions about a client and contain

details of conversations during a private counseling session or a group, joint, or family counseling session. Such notes are considered the therapist's personal notes and are not maintained in the client's health record, but are maintained separately by the therapist.

In most cases, including disclosure to another health care provider for treatment, payment or health care operations, psychotherapy notes can only be released with client authorization. However, authorization for the use or disclosure of psychotherapy notes is not required in the following circumstances:

- For use by the originator for treatment;
- For use in education programs including residency or graduate training programs;
- To defend a legal action brought by a client;
- For purposes of HHS determining compliance with the HIPAA Privacy Rules;
- As otherwise required by law;
- By a health oversight agency for a lawful purpose related to oversight of a psychotherapist;
- To a coroner or medical examiner for the purpose of identifying a deceased client, determining a cause of death, or other duties as required by law; or
- To law enforcement in instances of permissible disclosure related to a serious or imminent threat to the health or safety of a person or the public.

A client's right to request access to his/her health care records does not apply to psychotherapy notes maintained by a psychotherapist. The client's psychotherapist or physician must use professional judgment in determining whether a client should have access to psychotherapy notes.

Verification

DHHS agencies must obtain proper identification of all individuals, including clients, prior to allowing access to confidential information.

Agencies must establish and implement written procedures that are reasonably designed to verify the identity and authority of the requestor where the agency does not know the person requesting the information. Knowledge of a person may take the form of:

- A person known by the agency;
- A phone or fax number known by the agency;
- An address known by the agency; or
- A place of business known by the agency.

Where documentation, statements, or representations, whether oral or written, from the individual requesting individually identifiable health information is a condition of disclosure, the agency must obtain such documentation or representations prior to disclosing the requested information.

When the person requesting individually identifying health information is a public official, or a person

acting on behalf of a public official, the following procedures may be followed:

- If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status is sufficient.
- If the request is made in writing, the request should be on the appropriate government letterhead.
- If the request is made by a person who is acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of the agency such as contract for services, Memorandum of Understanding, or purchase order, that establishes that the person is acting on behalf of a public official.

Verification of the authority of a public official or a person acting on behalf of a public official may be managed in the following manner:

- A written statement of the legal authority under which the information is requested, or if a written statement would be impracticable, an oral statement of such legal authority; or
- If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

Agencies are required to verify the identity of anyone who is acting on behalf of a client or who is assisting in an individual's care before disclosing individually identifying health information. The client must identify anyone whom the client has authorized to receive the client's individually identifiable health information.

Incidental to an Otherwise Permitted Use and Disclosure

Certain incidental uses and disclosures are permitted if they occur as a by-product of another permissible or required use or disclosure.

Such use and disclosures must be considered secondary in nature that cannot reasonably be prevented, are limited in nature, and occurs as a result of another use or disclosure that is permitted by the HIPAA Privacy Rule. For example, if a client is in an examining room and overhears a doctor talking to another client about his treatment, this would constitute incidental access to the health information being discussed.

- Incidental use and disclosure is permitted only if the underlying use and disclosure DOES NOT violate the HIPAA Privacy Rule.
- Reasonable safeguards that have taken into account the size of the agency, the nature of information it holds, any potential risks to clients' privacy, and potential effects on clients' care and treatment must be in place to limit the instances of incidental use and disclosure.
- An incidental disclosure is not an accidental disclosure and does not have to be accounted for in the accounting of disclosures logs.

Limited Data Set (Research, Public Health or Health Care Operations)

A subset of paper or electronic records containing individually identifiable health information that excludes those elements that could identify a client may be disclosed to a recipient who has entered into a data use agreement with a DHHS agency. Use or disclosure of a limited data set may only be used for the purposes of:

- Research;
- Public health; or
- Health care operations.

A limited data set requires that all direct identifiers be removed not only for the client, but also the client's relatives, employers, or household members of the client. Disclosure of a code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified constitutes disclosure of individually identifiable health information.

De-identified information that has been re-identified shall be disclosed only as permitted in DHHS policies.

DHHS covered health care components may create a limited data set or may allow their business associate to create a limited data set; however, the component's business associate(s) may not disclose information in a limited data set without the DHHS agency's approval.

Other State and Federal Laws

DHHS agencies are required to evaluate state and other federal laws that apply to their programs to determine whether there is a requirement conflict between specific laws and to determine which state or federal law is the more stringent, thereby taking precedence for requirements. Agency procedures must reflect implementation requirements of the state and federal laws with which the agency must comply.

News Media

The DHHS Public Affairs Office is generally responsible for responding to the news media for agencies within the Department; therefore, agency procedures must ensure staff is knowledgeable about actions to be taken in responding to inquiries from the news media.

Chapter 16: Accounting of Disclosures

DHHS covered health care components shall, upon written request, provide clients or their personal representative with an accounting of disclosures of the client's individually identifying health information made by the component, including disclosures made by any of the agency's internal or external business associates, as appropriate.

Such accounting shall be for the time period requested up to six years prior to the request date, except as otherwise specified within this policy. The elements in the accounting and the provision of the accounting shall be consistent with all stipulations within this policy. DHHS covered health care components and internal business associates shall develop procedures for responding to requests by clients or their personal representatives for an accounting of the disclosures made about the client, and for ensuring the accountings are provided in a timely manner. Business Associate Agreements with external business associates shall include the requirement for providing the covered health care component with a listing of disclosures made by external business associates, upon request of the component.

For the purposes of this policy, 'disclosure' shall mean the release, transfer, provision of access to, or otherwise divulging of individually identifiable health information outside of the agency holding the information, and shall include disclosures made in *written, oral, or electronic* form.

DHHS covered health care components and internal business associates shall designate a staff member who is responsible for receiving requests for accounting of disclosures. It is strongly recommended that this responsibility be limited to one (1) person in the agency. Agencies are encouraged to designate a privacy official as the designated staff member. Each agency shall document the title of the staff member responsible for receiving and processing requests for an accounting. Documentation related to the designation of the staff member must be maintained for at least six (6) years.

Disclosure Exclusions/Inclusions

The types of disclosures listed below **do not** have to be included in the Accounting of Disclosures:

- Disclosures necessary to carry out treatment, payment, and health care operations such as:
- Disclosures to other health care providers (treatment);
- Eligibility, billing, claims management, medical necessity, and utilization review (payment); and

Provision of individually identifiable health information to the NC Office of the Attorney General when representing the interests of a covered component (health care operations).

NOTE: The definition of 'health care operations' is designed to identify those activities of a covered component that support the component's ability to provide treatment to individuals or to pay or be paid for such health care. Many disclosures that are required by law do not significantly further a covered entity's health care operations; rather, they further other important public purposes such as reporting child abuse, injuries due to violence, domestic violence or elder abuse, or responding to court orders.

- Disclosures made directly to the client who is the subject of the individually identifying health information or to the client's personal representative.
- Disclosures that are incidental to a use or disclosure that is otherwise permitted or required when covered components and business associates have implemented reasonable and appropriate administrative, technical, and physical safeguards to limit incidental, and avoid prohibited, uses and disclosures.
- Disclosures made pursuant to an authorization signed by the client or personal representative.
- Disclosures made to the facility's directory, to persons involved in the client's care, or for other permissible notification purposes Disclosures made for national security or intelligence purposes.
- Disclosures made to correctional institutions or law enforcement officials with lawful custody of an inmate if the individually identifying health information is necessary for:
 - The provision of health care to such clients;
 - Health and safety of the inmate or other inmates, officers, or other employees at the correctional institution;
 - Health and safety of clients and officers or others responsible for the transportation of inmates;
 - The enforcement of law within the correctional institution; and
 - The administration and maintenance of the safety, security, and good order of the correctional institution.

NOTE: Disclosures made to law enforcement officers who bring or pick up clients from the Division of Mental Health, Developmental Disabilities, and Substance Abuse Services (DMH/DD/SAS) facilities do not have to be included in the accounting.

- Disclosures of de-identified data or individually identifying health information that is part of a limited data set in accordance with DHHS Privacy Policy
- Disclosures that occurred prior to April 14, 2003.

Other than the exceptions noted above, all other disclosures of individually identifiable health information **must** be included in the accounting and may include any of the types of disclosures listed below.

- Public Health Authorities
- Surveillance
- Investigations
- Interventions
- Foreign governments collaborating with federal public health authorities
- Reporting vital events such as births and deaths
- Required reporting of diseases or injuries such as communicable diseases or registries such as cancer and immunization registries
- Social Services
- Child abuse, neglect, or exploitation
- Disabled adult abuse or neglect

Tracking Disclosures

Each DHHS covered health care component shall develop a process for documenting the accounting of disclosures. For those types of disclosures that must be tracked, such process must include tracking disclosures made by the component and their internal and external business associates of individually identifying health information that are disclosed either orally, on paper, or electronically. Disclosures may be tracked manually or in electronic form ensuring accurate and complete accounting of disclosures. Such process could include computerized tracking systems that have the ability to sort by individual and/or date or manual logs with one (1) log per client maintained in the client's medical record or other file. Each component shall ensure that appropriate staff and business associates receive training on the tracking process.

Each covered component shall determine if documentation of disclosures will be maintained in a centralized (e.g., all accountings maintained in a single database accessible to appropriate agency staff and business associates) or de-centralized fashion (e.g., each location that discloses information maintains an accounting for their location only). Such determination should be based upon complexity of the component and their internal and external business associates and the number of locations disclosing information that would have to be tracked.

If documentation of accounting of disclosures is de-centralized, the designated staff member shall identify all possible locations where disclosures may be made and where such accountings should be maintained; and shall ascertain if information about the client whose accounting is requested has been disclosed by any of the possible locations. It is the responsibility of the designated staff person to collect de-centralized accountings which may remain as many separate documents or be compiled into a single document.

When disclosures are made to a single source for multiple clients, it is not necessary to track each disclosure by making a notation in each medical record that has been accessed. The covered component need only document the following:

- The identity (and address if known) of the person/agency to which access was provided;
- A description of the records and individually identifiable health information to which the subject has access;
- The purpose for the disclosure; and
- When access was provided.

It would be sufficient, for instance, for the covered component to maintain a separate notation of such disclosures, applicable to all records so accessed. Then, if an individual requests an accounting, the covered entity need only determine whether the individual's records were among the universe of records to which the person/agency was granted access. All individuals whose records were accessed in this fashion would receive the same accounting for the disclosure. For example, retrospective review of medical records for all clients treated by a health care provider may be required to identify cases of new or previously unknown infectious agents. If a client requesting an accounting was treated by the health care provider during the period covered by the retrospective review, then the retrospective review should be included as part of the client's accounting.

If access to a universe of records is provided for a discrete period of time, the accounting can include the range of dates (e.g., access was provided from August 1 to August 3, 2003; or during the week of August 10, 2003). If the disclosure is routinely made within a set period from an event, the component is permitted to provide the date of the event and the normal interval (e.g., hospital discharges reported on 15th of the following month for all discharges during the month of June 2003).

Key features of an accounting of disclosures tracking system should include:

- Allowing data entry from anywhere in the component;
- Securing the information;
- Tracking usage and compliance throughout the component;
- Providing full auditing and reporting functionality;
- Ability to track all disclosures that must be accounted;
- Ability to track and report based on reason for disclosure;
- Providing for temporary suspension of accountings for disclosures to law enforcement officials or oversight agencies;
- Simplicity in using and understanding the process;
- Cost effective mechanisms; and
- The ability to provide on-demand accounting of disclosure reporting to the client or personal representative.

Request for Accounting of Disclosures

A client or personal representative's request for an accounting of disclosures must be made in writing. Each agency shall designate the person within the agency who will be responsible for receiving and processing all requests for an accounting. Agencies shall forward such requests to the designated person for action.

DHHS covered health care components shall develop and implement procedures for clients or their personal representatives to request an accounting of disclosures; and shall negotiate procedures with their internal and external business associates to coordinate requests for accountings disclosed by the separate agencies/work units.

Providing Accounting of Disclosures to Client or Personal Representative

Upon request, a client or personal representative shall be provided a written accounting of all disclosures of individually identifying health information made after April 14, 2003 by the covered health care component. Such accounting may include any period of time within the six years prior to the date on which the accounting is requested.

Covered health care components are required to act on a request for an accounting of disclosures within 60 days after receipt of the request. If the component cannot provide the accounting within 60 days, the component may extend the time to provide the accounting; however, only one 30-day extension is

permitted per request. Any extension requires the component to provide a written statement to the requester regarding the reason for the delay and the expected completion date.

DHHS agencies shall provide the client or personal representative's first request for an accounting at no charge to the client or personal representative. Agencies may charge the client or personal representative a reasonable, cost-based fee for any subsequent accountings within 12 months from the time the first request is received, provided that the fee includes only the cost of:

- Copying, including the cost of supplies for and labor of assembling and copying the information; and
- Postage, when the client has requested that the copy be mailed.

Exception: DMH/DD/SAS agencies are bound by 10A North Carolina Administrative Code (NCAC) 26B .0105 when determining fees for copying health information, including accountings of disclosure.

Agencies must inform the client or personal representative in advance of the fee and provide the client or personal representative with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. Adequate time shall be allowed for the client or personal representative to withdraw the request before incurring any costs.

Disclosures made to health oversight agencies or law enforcement officials shall be temporarily excluded from an accounting if the covered component has been notified by the oversight agency or law enforcement official that providing a client or personal representative with an accounting of the disclosures made to them could impede the progress of their activities (e.g., fraud investigation or investigation of possible criminal activities when a client should not be aware of such scrutiny). Such request from a health oversight agency or law enforcement official should be in writing; however an oral request may be accepted with stipulations, as noted below. Suspensions requested in writing shall remain in effect for the duration specified in the written request, unless the request for suspension is rescinded earlier by the health oversight agency or law enforcement official.

If a health oversight organization or law enforcement official requests this temporary suspension orally, the component shall perform the following:

- Document the statement, including the identity of the agency or official making the statement;
- Temporarily exclude from the accounting of disclosures those disclosures made to an oversight agency or law enforcement official based upon the oral information in the statement; and
- Limit the temporary exclusion to no more than 30 days from the date of the oral statement unless a written statement is submitted during that time specifying the duration.

Each component shall retain the following documentation for no less than six (6) years from the date the accounting request was received:

- Client or personal representative's request for an accounting;
- Copy of the accounting provided to the client or personal representative; and
- Title of the person or office responsible for receiving and processing accounting requests.

In the facilities operated by DMH/DD/SAS, the request for accounting and copy of the accounting provided to the client shall be maintained in the client's medical record. All other covered components shall determine the most appropriate location for maintaining the documentation.

Contents of the Accounting of Disclosures to Clients or Their Personal Representatives

Each accounting of a disclosure shall contain the following elements:

- The date of the disclosure;
- The name of the entity or person who received the individually identifying health information and, if known, the address of such entity or person;
- A brief description of the individually identifying health information disclosed; and
- Either:
 - A brief statement of the purpose of or reason for the disclosure that reasonably informs the client or personal representative of the basis for the disclosure;
 - A copy of any written request for disclosure by US DHHS for compliance purposes; or
 - A copy of a written request for a disclosure by a person or entity authorized to receive individually identifying health information for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (refer to DHHS Privacy Policy, Use and Disclosure Policies, Use and Disclosures).

Multiple Disclosures

If multiple disclosures are made to the same person or entity for a single purpose, either to the US DHHS for compliance purposes or for uses and disclosures for which consent, an authorization, or opportunity to agree or object is not required (refer to DHHS Privacy Policy, Use and Disclosure Policies, Use and Disclosures), the accounting should include the following:

- The elements listed in the 'Contents of the Accounting' shall be provided;
- The frequency, periodicity, or number of disclosures made to the common person or entity during the requested accounting period; and
- The date of the first and last disclosure made during the requested accounting period.

Research Disclosures

Disclosures for research purposes wherein authorization for use and disclosure of individually identifiable health information for research purposes has been waived or is not required must be included in the accounting of disclosures; however, disclosures for research purposes wherein authorization has been obtained for use and disclosure of such information do not have to be included in the accounting of disclosures.

If disclosures are made for 50 or more clients for research purposes, the accounting must include:

- The name of the research protocol activity;
- A plainly written description of the research protocol or activity, including:
 - Purpose for the research and
 - Criteria for selecting particular records to be disclosed for the research;
 - A brief description of the type of individually identifying health information that was disclosed;
 - The date or period of time during which the disclosures occurred, or may have occurred, including the date of the last such disclosure during the accounting period;
 - The name, address, and telephone number of the entity that sponsored the research, including the name of a contact person;
 - The name, address, and telephone number of the researcher to whom the information was disclosed; and
- An indication that the individually identifying health information of the client may or may not have been disclosed for the particular research protocol or activity.

If the component provides the modified content described above (in lieu of the standard content for an accounting), upon request by the client or personal representative, the component shall assist the client or personal representative in contacting the researcher if disclosures for research purposes were made by the component.

Due to the complexity of this policy and the involvement of numerous clinical, professional, clerical, and administrative staff, as well as business associates who must ensure disclosures are accounted for, each agency will need to develop a system for routinely monitoring compliance with this policy.

DHHS covered health care components must develop procedures that address the following processes for ensuring their clients' right to an accounting of disclosures of their health information. Procedures need to be coordinated between covered health care components and internal and external business associates.

- Designate the person(s) or office(s) responsible for receiving and processing requests for accounting of disclosures by clients or personal representatives.
- Develop training materials that ensure staff can differentiate disclosures that must be accounted for, from disclosures that do not have to be accounted for.
- Determine the acceptable method(s) for requesting and receiving an accounting.
- Develop an accounting request form.
- Identify all areas within the component and their business associates where disclosures that must be tracked would be made.
- Establish process to ensure required disclosures and accidental disclosures are routinely documented.
- Establish process for making reasonable efforts to provide accounting to clients or personal representatives within 60 days of request and process for one 30-day extension, if needed.
- Establish process for temporary suspension of certain accountings.

- Determine if agency will handle multiple disclosures or research disclosures differently from standard accountings.
- Ensure established process for accountings is correctly reflected in component's Notice of Privacy Practices.
- Determine any fees and a process for informing clients of the fee.
- Maintain audit trails that track client or personal representative requests for accountings.
- Develop process for monitoring compliance with policy.
- Maintain required documentation.

Chapter 15: DE-IDENTIFICATION OF HEALTH INFORMATION AND LIMITED DATA SETS

There are set methods that the North Carolina Department of Health and Human Services (NC DHHS) agencies may use to remove specific elements from health information so the resulting information will not be considered individually identifying health information. De-identified information can be used or disclosed without employing privacy protections.

An individual identifier is information that could reasonably enable the identification of a specific DHHS client or a relative, guardian, employer, or household members of that client. HIPAA Privacy Rule primarily addresses the protection of individually identifiable health information and specifies when such information can be used or disclosed. HIPAA allows a covered entity to de-identify health information by removing all identifying elements so that the remaining information cannot identify an individual and therefore is not subject to the protections specified for individually identifiable health information.

In addition to de-identifying health information, HIPAA permits the creation of a "limited data set" that can contain specific individual identifiers when such information is needed for public health, research, or health care operations activities and a "data use agreement" (DUA) has been executed. There are provisions in HIPAA, state laws, and other federal laws when individually identifying health information can be used and disclosed for public health, research, and health care operations without the necessity for a limited data set or data use agreement (e.g., public health disclosures required by law, licensure surveys). Therefore, data use agreements would only be needed for those public health, research, or health care operation uses and disclosures that are not otherwise permitted by federal or state laws.

DHHS agencies shall de-identify health information whenever individually identifying health information is not necessary to accomplish the intended purpose for the use or disclosure of health information or when use or disclosure of individually identifying health information is not permitted by federal or state laws.

DHHS agencies shall comply with all conditions in this policy regarding the creation, use, and disclosure of health information for which the elements that could reasonably be expected to identify a specific individual have been removed or restricted to a limited data set. Each DHHS agency that is a recipient of a limited data set must sign a data use agreement and shall comply with the conditions of that agreement. A DHHS agency may use the limited data set for its own activities or operations provided that the information used is the minimum necessary to accomplish the intended purpose.

This policy shall apply to *paper* documents as well as *electronic* data in any form (e.g., paper or electronic records, system data, tape, disc, etc.)

When information cannot be de-identified or included in a limited data set, the agency shall ensure that disclosure of the health information is permitted by law and is in accordance with DHHS Privacy Policies.

Individual Identifiers

For the purposes of DHHS Privacy Policies, the following elements are considered individual identifiers if they apply to DHHS clients or relatives, guardians, employers, or household members of DHHS clients. If

the elements below are associated with health information, the information becomes individually identifying health information that must be protected from improper use or disclosure:

- Names
- All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes, except for the initial (3) three digits of a zip code if, according to the current publicly available data from the bureau of the census:
- The geographic unit formed by combining all zip codes with the same three (3) initial digits contains more than 20,000 people; and
- The initial three (3) digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security Numbers (SSN);
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that can be re-identified

De-Identification

Individually identifiable health information is de-identified when elements have been removed that could identify an individual and there can be no reasonable basis to believe that the information may be used, with or without other available information, to identify an individual. De-identified health information may be used and shared as necessary in the performance of an agency's work, unless the information is otherwise restricted by federal or state laws.

Such health information may be considered de-identified only if the following criteria are met:

- The agency is unaware of a means by which the information could be used alone or in combination with other information to identify an individual who is the subject of the information; and a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (e.g., statistician I or II):
- Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is the subject of the information; and
- Documents the methods and results of the analysis that justify such determination; or
- The identifiers (listed above) of the client or relatives, guardians, employer, or household members of that client are removed.

An agency may engage a business associate to serve as the qualified person with "appropriate knowledge and experience with generally accepted statistical and scientific principles and methods" to de-identify information. (Note: Several DHHS divisions, facilities and schools employ individuals with statistical background/experience who may be able to provide this type of service.) The use of the disclosed data and the recipients of the data shall be considered in the risk assessment conducted by the qualified person. An agency that uses an internal or external person to satisfy this de-identification criteria shall develop a procedure to verify that the individual adequately meets the knowledge and experience criteria.

Health information that has been considered de-identified does not meet the de-identification criteria if either of the following is true:

- A code or other means of record identification designed to enable coded or otherwise de-identified information to be re-identified is provided; or
- De-identified information is re-identified.

Limited Data Set

DHHS agencies may use or disclose individually identifying health information that contains a limited number of identifiers (i.e., *limited data set*) for public health, research, or health care operation activities whenever the limited data set will meet the intended purpose for the use or disclosure. When a limited data set is deemed appropriate for a use or disclosure, DHHS agencies will enter into a data use agreement, using a DHHS Data Use Agreement, with the recipient of the information unless the use or disclosure is permitted by state or federal law, which negates the need for such an agreement.

When limited data sets are used or disclosed with an appropriate data use agreement executed:

- An authorization is not required for the use or disclosure of a limited data set; and
- Limited data sets do not need to be included in an accounting of disclosures.

To qualify as a limited data set, the following identifiers for DHHS clients or relatives, guardians, employers, or household members of those clients can be associated with health information:

- State, county, city or town, zip code, SSN;
- Birth date, admission date, discharge date, date of death;
- Age; and/or
- Unique identifying number, characteristic, or code exclusive of identifiers such as SSN, account numbers, medical record numbers, etc., as listed in the Exclusion of Data Elements section below.

Exclusion of Data Elements Considered to be Identifying Elements

The table below outlines the identifiers that must be **excluded** from individually identifying health information in order to consider the information as de-identified or as a limited data set. (See [Appendix A](#) for a list of all elements that can be **included** in de-identified information or a limited data set.)

DATA ELEMENTS THAT MUST BE <u>EXCLUDED</u> TO BE CONSIDERED DE-IDENTIFIED DATA OR A LIMITED DATA SET		
ELEMENTS	DE-IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
Names of clients or employers, household members, guardians, or relatives of clients	X	X
Street address or post office box number of clients or employers, household members, guardians, or relatives of clients	X	X
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients	X	
State of clients or employers, household members, guardians, or relatives of clients		
First three (3) digits of the zip code of clients or employers, household members, guardians or relatives of clients if , according to the Bureau of Census, the population of all zip codes with the same first three (3) digits is greater than 20,000 people . E.g., If the population of all zip codes that begin with 276 is more than 150,000, you can include 276 in de-identified health information.		
First three (3) digits of the five digit zip code of clients or employers, household members, guardians or relatives of clients if , according to the Bureau of Census, the population of the all zip codes with the first three (3) digits is less than 20,000 people . E.g., The total population for all zip codes starting with 211 - say 21101 and 21104 - is 19,200 people. In this case, you could not use the first three (3) digits of the zip code in de-identified health	X	

information.		
Last two (2) digits of the zip code of clients or employers, household members, guardians or relatives of clients	X	
Five (5) digit zip code of clients or employers, household members, guardians, or relatives of clients. E.g., the five (5) digit zip code of 27603 must be excluded from de-identified data, but can be included in a limited data set.	X	
Dates exclusive of year (e.g., month/day) directly related to a client including admission date, discharge date, date of death	X	
Birth date exclusive of year (e.g., month/day) for clients age 89 and under	X	
Birth date inclusive of year (e.g., Month/Day/Year) for clients age 90 and above (not aggregated - e.g., 1880-1913)	X	
Age 89 and under		
Specified ages 90 or above (not aggregated - e.g., 90+)	X	
Telephone numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Fax numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Electronic mail addresses of clients or employers, household members, guardians, or relatives of clients	X	X
SSN of clients or employers, household members, guardians, or relatives of clients	X	X
Medical record numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Health plan beneficiary numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Account numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Certificate/license numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Vehicle identifiers and serial numbers , including license plate numbers, of clients or employers, household members, guardians, or relatives of clients	X	X
Medical device identifiers and serial numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Web Universal Resource Locators (URLs) of clients or	X	X

employers, household members, guardians, or relatives of clients		
Internet Protocol (IP) address numbers of clients or employers, household members, guardians, or relatives of clients	X	X
Biometric identifiers , including finger and voice prints of clients or employers, household members, guardians, or relatives of clients	X	X
Full face photographic images and any comparable images of clients or employers, household members, guardians, or relatives of clients	X	X
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the <i>Re-Identification</i> section of this policy)	X	
Gender, race, ethnicity, or marital status		

Re-Identification

An agency may assign a code or other means of identification to allow information that has been de-identified to be re-identified within the agency, provided that:

- The code or other means of identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual (examples would be codes containing a SSN or the unique ID algorithm assigned to clients served in facilities operated by the Division of Mental Health, Developmental Disabilities, and Substance Abuse Services);
- The agency does not use or disclose the code (or other means of identification) for any purpose other than that originally intended; and
- The agency does not disclose any methods that can be used to re-identify information that has been de-identified.

Data Use Agreement

DHHS agencies that use or disclose a limited data set, wherein the use or disclosure is not permitted by state or federal law, the agency shall enter into a data use agreement with the limited data set recipient(s) consistent with a DHHS Data Use Agreement provided by the department. The data use agreement must contain the following:

- A requirement to use or disclose such information only for the purposes of research, public health, or health care operation activities;
- Specifications regarding who can use or receive the limited data set;
- Specifications of the permitted uses and disclosures;

- A stipulation that the recipient will not use or disclose the limited data set for any purposes other than those specified in the data use agreement or as otherwise required by law;
- Adequate assurances that the recipient will use appropriate safeguards to prevent the use or disclosure of the limited data set for any purposes other than those specified in the data use agreement. These assurances may be addressed through language similar to that provided in a DHHS Data Use Agreement;
- Commitment by the recipient to report to the agency any use or disclosure of the information not provided for by the data use agreement of which it becomes aware;
- Assurance that any agent, including a subcontractor, to whom the recipient provides the limited data set agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information; and
- A commitment by the recipient that they will not re-identify the information or contact any of the individuals whose data is being disclosed.

If an agency staff member becomes aware of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the recipient's obligation under the data use agreement, the staff member shall notify that agency's privacy official who shall take reasonable steps to cure the breach or end the violation. If unsuccessful, the agency privacy official shall ensure that disclosure of limited data sets to the recipient is discontinued. The agency privacy official shall report the problem to the DHHS Privacy Officer, who will determine if further actions are warranted which could include reporting the material breach to the Secretary of the US Department of Health and Human Services.

The minimum necessary rule shall apply to limited data sets; therefore, only data elements that are necessary to perform the purpose(s) specified in the data use agreement should be included in the limited data set released to the recipient.

Implementation Activities

Each agency shall identify those areas within the agency that may use or disclose health information that includes any of the identifiers specified in this policy for purposes other than treatment or payment or when authorized by the client. Each agency shall ensure that staff in these areas understand:

- The elements that constitute identifiers;
- The potential for use or disclosure of limited data sets when data use agreements are in place; and
- That there are specific laws that must be adhered to when using or disclosing individually identifying health information.

A business associate who has entered into an approved Business Associate Agreement with the DHHS agency may be engaged for the purpose of converting individually identifiable health information into de-identified health information or a limited data set.

Each agency shall develop a procedure to ensure compliance with this policy regarding de-identified health information and limited data sets. This procedure shall include oversight, which may be centralized and/or may include a committee review, as well as procedures for coding and re-identifying individually identifying health information that are in accordance with the coding requirements in this policy.

If time constraints prohibit the immediate creation of de-identified health information, these circumstances shall be documented and provided to the agency privacy official. When practicable, these issues shall be resolved to enable de-identification for future comparable occurrences.

Appendix A - Elements Permitted in De-identified Health Information and Limited Data Sets

The table below lists the elements that can be included in de-identified health information. The table also identifies those data elements, including some individual identifiers that are allowed to be included in a limited data set. Note that the individual identifiers that can be included in a limited data set are not likely to identify an individual if no additional individual identifiers are used.

IDENTIFYING DATA ELEMENTS THAT CAN BE INCLUDED IN DE-IDENTIFIED DATA OR A LIMITED DATA SET ('X' indicates that the element can be included)		
ELEMENTS	DE-IDENTIFIED ELEMENTS	LIMITED DATA SET ELEMENTS
ADDRESS		
County, city, town, or precinct of clients or employers, household members, guardians, or relatives of clients		X
State of clients or employers, household members, guardians, or relatives of clients	X	X
First three (3) digits of the zip code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the combined population of all zip codes with the same first three (3) digits is greater than 20,000 people	X	X
First three (3) digits of the five (5) digit zip code of clients or employers, household members, guardians or relatives of clients if, according to the Bureau of Census, the combined population of the all zip codes with the first three (3) digits is less than 20,000 people		X
Five (5) digit zip code of clients or employers, household members, guardians, or relatives of clients		X
DATES		
Year of client-related dates , including admission date, discharge date, and date of death	X	X

Dates exclusive of year (month/day) directly related to a client, including admission date, discharge date, and date of death		X
Year of birth for clients age 89 and under	X	X
Year of birth for clients age 90 and above		X
Aggregated years of birth for clients age 90 and over (e.g., 1880-1913)	X	X
AGE		
Age 89 and under	X	X
Ages 90 or above (not aggregated - e.g., 90 or 98)		X
Aggregated ages , including ages 90 and over (e.g., 5-15 or 90-105)	X	X
OTHER		
Any other unique identifying number, characteristic, or code (unless such code is developed in accordance with the <i>Re-Identification</i> section of this policy) that is not one of the following : SSN Medical record number Account numbers Certificate/license numbers IP address numbers Telephone number Vehicle IDs/serial numbers Medical device IDs/serial numbers Health plan beneficiary number Fax numbers		X
Gender, race, ethnicity, or marital status	X	X

Chapter 16: MINIMUM NECESSARY

DHHS agencies, must make reasonable efforts to limit individually identifiable health information to that which is *minimally necessary* to accomplish the intended purpose for the use, disclosure, or request for information. DHHS agencies must evaluate their current practices for using and disclosing individually identifiable health information in order to enhance protections, as needed, to limit unnecessary or inappropriate access to individually identifiable health information.

The minimum necessary requirement applies to:

- Uses or disclosures for payment or health care operations;
- Uses or disclosures requiring the client to have an opportunity to agree or object;
- Uses or disclosures that are permitted without the client's permission
- (except for those required by law or specified; and
- Uses or disclosures by External Business Associates.

Controlling the "use" of individually identifiable health information that is **primarily paper-based** within an agency presents special challenges in applying the minimum necessary requirements. Agencies must rely heavily on the development and implementation of policies and procedures, as well as self-policing. Therefore, this policy takes on special importance for agencies maintaining individually identifiable health information on paper (e.g., paper client records and diagnostic images).

Minimum Necessary within Agency

DHHS agencies are required to identify persons or classes of persons in its workforce who need access to individually identifiable health information and the categories of information to which access is needed.

DHHS agencies must develop and implement procedures that limit routine disclosures of individually identifiable health information to the amount reasonably necessary to achieve the purpose of the disclosure.

DHHS agencies are required to develop criteria designed to limit individually identifiable health information to the minimum necessary.

Minimum Necessary Outside Agency

DHHS agencies may rely on a request for disclosure as being limited to the individually identifiable health information that is minimally necessary, if:

- Disclosure is to a public official who represents that the request is for the minimum necessary information;
- The request is from another HIPAA covered health care component;
- The request is from a professional in the agency's own workforce or from a business associate, and the professional represents that the request is for the minimum necessary information; or
- The requestor provides documentation that the disclosure is for research purposes.

The minimum necessary requirement **does not** apply to:

- Disclosures to or requests by a health care provider for treatment;
- Uses or disclosures made to a client to whom the information applies;
- Uses or disclosures authorized by the client (or the client's personal representative);
- The Secretary of the United States Department of Health and Human Services for compliance enforcement;
- Uses or disclosures required by law; or
- Uses or disclosures required for compliance with the HIPAA Privacy Rule.

IMPLEMENTATION

The following protocols are in compliance with the HIPAA Privacy Rule and should be considered when staff share individually identifiable health information in the performance of their job responsibilities and when sharing individually identifiable health information with individuals outside the agency.

When using individually identifiable health information within an agency, DHHS agencies must categorize users by their "need-to-know" in order to accomplish their job responsibilities and establish standard protocol (criteria) that *reasonably* limits inappropriate access to individually identifiable health information based on the following categories:

Standard Protocol for Uses of Individually Identifiable Health Information by an Agency's Own Workforce

- For uses of individually identifiable health information by its own workforce within the agency, standard protocol must:
 - Identify the persons or groups of persons who need access to individually identifiable health information to carry out their job functions;
 - Identify the type of individually identifiable health information to which each person or group needs access, as well as the conditions under which they need the access; and
 - Make reasonable efforts to limit the access of its staff to only the information appropriate to their job functions.
- Standard Protocol for Disclosures of Individually Identifiable Health Information by an Agency's Own Workforce

For routine, recurring disclosures of individually identifiable health information by an agency's own workforce, standard protocol must:

- Identify the types of information to be disclosed;
- Identify the types of persons who would receive such information;
- Identify the conditions that would apply to such access; and
- Develop reasonable criteria for disclosures to routinely hired types of business associates (e.g., medical transcription).

For ***non-routine disclosures*** of individually identifiable health information by an agency's own workforce, standard protocol must:

- Develop reasonable measures to limit information to the minimum necessary to accomplish the purpose of the disclosure; and
- Use these measures to review non-routine disclosures on an individual basis.

Standard Protocol for Making Requests for Individually Identifiable Health Information by an Agency's Own Workforce

For ***routine, recurring requests*** for individually identifiable health information by an agency's own workforce, standard protocol must:

- Describe what information is reasonably necessary for the purpose of the request; and
- Limit the request for individually identifiable health information to that information.

For ***all other requests*** for individually identifiable health information by an agency's own workforce, standard protocol must ensure that each request is reviewed by an agency staff member who has authority to determine that the information requested is limited to what is reasonably necessary to accomplish the purpose of the request.

Criteria must be developed that control both the request for, and the disclosure of, **the entire client record**. Criteria must specifically justify why the entire client record is required. Exceptions to agency criteria are prohibited without prior approval of the Agency Privacy Official.

Individuals or entities external to the Department that perform activities or functions on behalf of a DHHS covered health care component as defined by the HIPAA Privacy Rule, are considered **External Business Associates** of a DHHS agency. As such, External Business Associates are required to comply with the Minimum Necessary requirement as specified in the HIPAA Privacy Rule.

The minimum necessary policy is intended to make DHHS agencies evaluate their current procedures and enhance protections needed to limit unnecessary or inappropriate access to and disclosures of, individually identifiable health information.

Chapter 17: RESEARCH

HIPAA Privacy Rule establishes the conditions under which individually identifiable health information may be used or disclosed by covered health care component and their internal business associates for research purposes. Research is defined in the privacy rule as “a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.” The HIPAA definition of research also applies to the development of research repositories and research databases. For the purposes of this policy, this definition of research is expanded for institutions operated by the Division of Mental Health, Developmental Disabilities and Substance Abuse Services (DMH/DD/SAS) to include the definition of research provided in North Carolina Administrative Code (NCAC), 10A NCAC 28A.0102, in which “‘research’ means inquiry involving a trial or special observation made under conditions determined by the investigator to confirm or disprove an [sic] hypothesis or to explicate some principle or effect.”

The privacy rule also defines the means by which clients will be informed of uses and disclosures of their individually identifying health information for research purposes, and their rights to access their health information held by covered health care components and internal business associates. Where research is concerned, the privacy rule protects the privacy of individually identifiable health information, while at the same time ensuring that researchers continue to have access to medical information necessary to conduct vital research.

DHHS agencies conducting research on clients shall have access to an Institutional Review Board established in accordance with the Common Rule (45 CFR 46, Subpart A) that will:

- Review and modify, disapprove, or approve research protocols and informed consent for research forms; and
- Conduct periodic reviews of the research.

DHHS researchers shall request the individually identifying health information that is the minimum necessary to conduct the research. Whenever possible, DHHS researchers shall request either de-identified data or a limited data set as necessary if either of these is the minimum necessary for conducting the research.

Each DHHS researcher that is a recipient of a limited data set shall sign a data use agreement with the DHHS agency that maintains the information and shall comply with the conditions of that agreement, in accordance with the DHHS policies.

Each DHHS researcher that receives individually identifiable health information from a DHHS covered health care component or internal business associate shall ensure that the information is protected in accordance with the DHHS Privacy Policies.

The requirements in this policy are in addition to (not a replacement for) other policies and regulations for human subjects research.

For treatment purposes, DHHS covered health care components shall contact researchers (either internal or external to DHHS) if a research subject seeks additional health care services from or is admitted into the component for additional treatment.

Researchers External to DHHS

DHHS agencies that receive requests for individually identifying health information from researchers external to DHHS shall require the researcher to submit the request in writing. Research requests must be documented in accordance with the requirements identified in this policy.

Institutional Review Boards

Institutional Review Boards (IRBs) are responsible for reviewing and modifying (to secure approval), disapproving, or approving the following for research involving human subjects:

- Research protocols;
- Forms to be used by researchers to obtain authorizations for the use or disclosure of client's individually identifying health information for research;
- Forms to be used by researchers to obtain informed consents from research subjects;
- Requests to waive or alter the requirement for client informed consent for participation in research study; and
- Requests to waive or alter the requirement for client authorization for the use or disclosure of client individually identifying health information for research.

DHHS agencies conducting research involving human subjects shall either:

- Establish an internal IRB in accordance with the Common Rule as necessary to review, approve, and monitor such research; or
- Identify an IRB external to DHHS that will review, approve, and monitor such research.

DHHS IRBs shall implement and document procedures for normal review as defined in 45 CFR 46.108(b), or expedited review according to the procedures defined by 45 CFR 46.110.

DHHS IRBs shall document all decisions regarding the modification, approval, or disapproval of research protocols, documentation, and requests to waiver or alter the informed consent or authorization requirements. The IRB shall also record meeting minutes and document continuing review activities.

These records shall be maintained for a minimum of three (3) years, as required by 45 CFR 46.115.

Research Conducted with Client Authorization

Unless otherwise permitted by this policy, or required by state or federal law, a client authorization must be obtained prior to the use or disclosure of the subject's individually identifiable health

information for research purposes. Any authorization form received by a DHHS agency from a researcher external to DHHS must contain the following elements to be considered valid:

- A specific and meaningful description of the information to be used or disclosed;
- The name of the entity (e.g., Dorothea Dix Hospital) authorized to disclose the individually identifying health information for research purposes;
- The name of the researcher or entity conducting the research to whom the disclosure of individually identifying health information for research purposes can be made;
- A description of the specific research study in which the information will be used (authorizations cannot be used for nonspecific research or future, unspecified projects);
- An expiration date or event (e.g., client discharge) for the authorization that relates to the client or the research. The following statements meet the requirements for an expiration date or an expiration event if the appropriate conditions apply:
 - The statement “end of the research study” or similar language;
 - The statement “none” or similar language if the purpose of the authorized disclosure of individually identifying health information is for the researcher to create and maintain a research database or repository;
- Signature of the client and the date of the signature. If a client’s personal representative signs the authorization form, a description of the personal representative’s authority to act on behalf of the client must also be provided.

An authorization is always required for access, disclosure, or use of psychotherapy notes for research purposes. An authorization for access, use, or disclosure of psychotherapy notes for research may not be combined with any other authorization except other authorization for access, disclosure, or use of the same notes.

If a client elects to revoke his/her authorization for the use and disclosure of individually identifying health information for research purposes, the revocation must be documented on the original authorization form in the Revocation section. This revocation shall become a permanent part of the research record and the client’s medical record. Researchers within DHHS shall report the revocations to the institutional review board at the time of continuing review.

DHHS agencies shall provide a copy of the signed research authorization to clients or their personal representatives.

NOTE: Client authorization for use and disclosure of individually identifiable health information for research purposes does not replace the informed consent to participate in a research study required by the Common Rule, the FDA Protection of Human Subjects Regulations, NCGS 122C-57 (f), 10A NCAC 26C.0200, 10A NCAC 26D.1300, or 10A NCAC 28A.0305.

Alteration or Waiver of Client Authorization to Use or Disclose Individually Identifying Health Information for Research

A DHHS researcher may submit a request to an IRB or privacy board for a waiver or alteration of client authorization for the use or disclosure of individually identifying health information for research if the researcher determines that obtaining client authorizations is not feasible. For example, a researcher may need to request an alteration or waiver of requirement for client authorization for the use or disclosure of individually identifying health information for research in the following cases:

- The researcher cannot practicably obtain a potential research subject's authorization for the review of individually identifying health information in advance of contacting the potential subject; or
- The research will only involve the use of existing client records or specimens and no intervention, interaction, or direct contact of any kind with the research subjects will occur.

In the first case, an IRB or privacy board may elect to approve the researcher's request for a limited waiver of authorization that will permit specified access and use of individually identifying health information solely for prescreening and recruitment contact pursuant to the approved research protocol. In the second case, the volume and/or age of records to be examined during the research may be such that it would not be practicable for the researcher to obtain client authorization beforehand. If the risk to the client's privacy is minimal, the IRB or privacy board may also elect to approve a waiver in this instance.

DHHS researchers shall submit all requests for the alteration or waiver of client authorizations for research in writing to an institutional review or privacy board.

If the IRB or Privacy Board approves the request for alteration or waiver of client authorization, the board shall document that the following criteria are satisfied:

The documentation of the alteration/waiver of authorization approval shall also include the following elements:

- A statement identifying the IRB or the privacy board and the date on which the alteration or waiver was approved;
- A brief description of the individually identifiable health information for which use or access has been determined by the IRB or the privacy board to be necessary to the research;
- A statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited procedures; and
- A signature from the chair of the IRB or privacy board, or from another member of the board who has been designated by the chair.

If a DHHS IRB or privacy board does not approve a request to alter or waive the client authorization requirement for research, the board must inform the researcher of the decision in writing. Similarly, if

the board requires a change to the request for the alteration or waiver of client authorization prior to approving the request, the required changes must be documented and sent to the researcher.

If a research project is taking place at multiple sites and/or requires the use and disclosure of individually identifying health information created or maintained by more than one agency (collectively referred to as 'multisite projects'), more than one IRB may be involved in research study reviews, or researchers participating in the multisite project may elect to use a single IRB. The same situation is expected to occur with Privacy Boards. In some circumstances, Privacy Boards and IRBs will coexist. Regardless, a DHHS agency may rely on a waiver or an alteration of authorization approved by any IRB or Privacy Board, without regard to the location of the approver. However, DHHS agencies may elect to require duplicate IRB or Privacy Board reviews before disclosing individually identifying health information to requesting researchers.

Researchers external to DHHS covered health care components that identify potential research subjects during their reviews preparatory to research must submit a written request to the DHHS agency if they want the agency to notify the client about a possible opportunity to participate in the research.

DHHS researchers that are part of the DHHS covered health care component's workforce may contact the client directly for the purposes of recruitment for the research study. However, DHHS researchers must obtain authorization from a client who has indicated interest in participating in a study prior to asking the client any screening questions that involve individually identifying health information.

NOTE: If the preparatory research activity involves human subjects research (e.g., research subject recruitment, prescreening), the preparatory research activity must be reviewed and approved by an IRB and must satisfy the informed consent requirements unless otherwise waived by an IRB.

Health information may be considered de-identified if one of the following criteria is met:

The DHHS agency is unaware of a means by which the information could be used alone or in combination with other information to identify a client who is the subject of the information; **and** a person with appropriate knowledge and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable (e.g., Statistician I or II):

- Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify a client who is the subject of the information; and
- Documents the methods and results of the analysis that justify such determination.

The following identifiers for the client or the relatives, guardians, employer, or household members of that client are removed:

- Names;

- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geocodes, except for the initial three digits of a ZIP Code if, according to the current publicly available data from the Bureau of the Census:
- The geographic unit formed by combining all ZIP Codes with the same three initial digits contains more than 20,000 people; and
- The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000;
- All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
- Telephone numbers;
- Facsimile numbers;
- E-mail addresses;
- Social Security Numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic, or code that can be re-identified without the use of the code key or knowledge of the method used to re-identify the information.

Use of Limited Data Sets in Research

DHHS agencies may use or disclose a limited number of individual identifiers via a 'limited data set' for research without client authorization or IRB/Privacy Board alteration or waiver of authorization whenever the limited data set will meet the researcher's request.

To qualify as a limited data set, only the following identifiers for DHHS clients or relatives, guardians, employers, or household members of those clients can be associated with the health information:

- State, county, city or town, and/or ZIP Code;
- Birth date, admission date, discharge date, and/or date of death;
- Age; and/or
- Any unique identifying number, characteristic, or code, except for the following:
 - Social Security Numbers;

- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers; and
- Device identifiers and serial numbers.

All other individual identifiers such as name, address, telephone number, etc. must be removed from the data before the resulting information can be considered a limited data set.

Research Requests Received from Organizations External to DHHS

All requests for access to health information (e.g., individually identifying health information, limited data sets, de-identified health information) for research purposes, including those from researchers external to DHHS, must be submitted in writing to DHHS agencies via the Request for Access to Data form. In addition to the *Request* form, researchers must submit the following documentation, as indicated on the form for their type of request:

Research protocol;

- IRB approval letter for the research protocol;
- Informed consent forms for research signed by DHHS clients that have agreed to participate in the research study as subjects, or IRB approval of informed consent alteration or waiver;
- Either:
 - Authorization forms signed by DHHS clients that have agreed to become research subjects;
 - IRB/Privacy Board approval of client authorization alteration or waiver; or
 - Request that the DHHS agency obtain client authorization Upon DHHS agency request, documentation of the decedent status of the clients who is the subject of the individually identifying health information requested. (NOTE: If the researcher does not specify clients, but requests individually identifiable health information for “deceased clients” in general, then the DHHS covered component will not need to request proof of client death.)

DHHS researchers may disclose individually identifying health information that has been gathered or created during the research study if the disclosure is:

- Permitted by client authorization;
- Permitted by the approved alteration or waiver of authorization;
- Permitted by the data use agreement;
- Made to the sponsor of the study if the protocol includes a FDA regulated product or activity for which the sponsor is responsible, and the disclosure is for the purposes of quality, safety, or effectiveness (e.g., adverse event/safety reports for investigational new products);

- Made to a health oversight agency that is performing oversight activities authorized by law (e.g., disclosure to the Office for Human Research Protections for the purposes of determining compliance with the Common Rule); or
- Required by law (e.g., disclosure to cancer registries, other public health reporting).

If a revision to the authorization or alteration/waiver of authorization is necessary to allow the desired disclosure, an IRB or Privacy Board must approve the revision to the protocol. If the terms of the data use agreement must be changed to permit the disclosure, a revised data use agreement must be signed by the researcher and the covered component.

Individually identifying health information gathered during the research study may not be included in presentations or publications of any type unless explicitly permitted by:

- The client via authorization or informed consent for research;
- Waiver of the client's authorization by an IRB or Privacy Board;
- Waiver of the client's informed consent by an IRB; or
- The data use agreement signed by the DHHS agency disclosing the health information and the researcher.

DHHS agencies may not allow the authorization, alteration/waiver of authorization, or data use agreement obtained for one research project to be used for another research project. However, the IRB or Privacy Board may reanalyze such disclosures and grant a waiver for other studies.

Retention of Research Documentation

DHHS agencies receiving requests for access to individually identifying health information for research shall maintain a copy of the following in the client records:

- The approved request for access to health information for research. The research protocol and IRB letter of approval;
- Client authorization or IRB/Privacy Board documentation of approved alteration/waiver of authorization; and
- Client informed consent or IRB documentation of approved alteration/waiver of informed consent.

Research documentation filed in the client record must be retained according to the agency's retention and disposition schedule for such records.

DHHS researchers must maintain copies of authorizations for research and approved waivers of authorization for a minimum of six (6) years from the date of creation, or the date on which the document was last in effect, whichever is later.

Accounting of Disclosures of Individually Identifying Health Information for Research Purposes

Clients have a right to request access to an accounting of all disclosures of their individually identifying health information for research purposes, unless such disclosure was made:

- Pursuant to the client's authorization; or
- As part of a limited data set.

Similarly, clients will not receive an accounting of disclosures of their health information if the information was de-identified.

Documentation of disclosures must be kept in the circumstances listed below and provided to clients upon their request:

- Disclosures pursuant to an IRB or Privacy Board alteration or waiver of authorization;
- Disclosures used in preparation of a research protocol; or
- Disclosure of a decedent's individually identifying health information used for research.

Chapter EIGHTEEN: MARKETING AND FUNDRAISING

'Marketing' is defined as a communication about a product or a service, the purpose of which is to encourage clients to purchase or use the product or service. The following are examples of communications that are NOT considered marketing:

- Describing a product or service provided by the agency;
- Reviewing treatment with a client;
- Discussing case management or coordination of care; and
- Recommending alternative treatments.

'Fundraising' is defined as an organized activity of raising funds for an agency cause, including appeals for money and sponsorship of events.

DHHS agencies shall not disclose individually identifiable health information about clients without authorization for marketing or fundraising purposes. Such authorization must include the specific reason for using the client's information.

Agencies shall not disclose, sell, or coerce a client to permit disclosure of individually identifiable health information for marketing purposes without the authorization of the client who is the subject of the confidential information or the client's personal representative. This prohibition includes the disclosure, use, or selling of prescription drug patterns.

Exception: DHHS agencies must obtain an authorization for marketing except when the communication is in the form of:

- Face-to-face communication made by an agency to a client or
- Promotional gift of nominal value provided by DHHS.

This provision allows agencies to discuss products or services as well as provide sample products without restriction.

The health care services listed below are common communications that a client generally expects to receive as part of his/her continued health care services and are not considered marketing.

- Disease management
- Wellness programs
- Prescription refill reminders
- Appointment reminders

Agencies performing fundraising activities, including appeals for money and sponsorship of events, may internally **use** only dates of treatment and demographic information, unless the client or the client's personal representative gives authorization for more expansive use of the client's individually identifiable health information. Demographic information that may be disclosed without authorization typically includes:

- Name;
- Address;
- Other contact information;
- Age;
- Gender; and
- Insurance status.

Disease-related information such as diagnosis may not be used in fundraising. In addition, information about the component from which a client received services also cannot be used for fundraising purposes without the client's authorization if that information could reveal the nature of the diagnosis, service, or treatment the client received.

Agencies that allow clients to participate in fund-raising activities (e.g., raffle to raise funds to help pay for an off campus trip for a patient care unit) must ensure that the client's participation is voluntary. For incompetent clients, authorization from the client's guardian is required before the client can participate in such fund-raising activities.

Agencies may **disclose** a client's dates of treatment and demographic information for fundraising purposes without the client's authorization only as follows:

- To a covered health care component's business associate, pursuant to a business associate agreement;
- To an agency-related foundation, unless prohibited by law;
- The agency has included in their "Notice of Privacy Practices" that a client's individually identifiable health information may be used or disclosed for fundraising purposes;
- When clients are sent fundraising materials that include a description of how the client may opt-out from receiving any further fundraising communications; and
- Reasonable efforts have been made to ensure that clients who decide to opt-out from receiving future fundraising materials are not sent any materials from that point forward.

DHHS agencies that are engaged in marketing or fundraising activities must ensure that the requirements listed below are met.

Authorizations

An authorization for the purposes of marketing and fundraising must state that the purpose of the disclosure is for marketing or fundraising activities and denote whether the individual's health information will be disclosed to a third party.

Fundraising materials must describe how an individual may opt-out of receiving any further fundraising communications. Covered health care components must document a process for fulfilling those requests.

CHAPTER NINETEEN: RIGHTS OF CLIENTS

DHHS agencies shall establish and implement procedures that ensure the following rights of clients as delineated by the HIPAA privacy rule and other federal and state laws.

- Right to Confidential Communications
- Right to Adequate Notice of Use and Disclosure of Individually Identifiable Health Information
- Right to Obtain Paper Copy after Electronic Notice
- Right to Request Access/Inspect/Copies of Individually Identifiable Health Information
- Right to Request Amendment to Individually Identifiable Health Information
- Right to Accounting of Disclosures of Individually Identifiable Health Information
- Right to Request Privacy Restrictions for Individually Identifiable Health Information
- Right to a Contact Person to Whom Client May Lodge Privacy Complaint

The rights that are included in this policy apply to individuals served by DHHS health care providers and health plan recipients, unless otherwise specified. For simplification purposes, this policy shall refer to all such individuals as 'clients', unless there is a difference in policy requirements.

The personal representative of a client who is acting on behalf of that person is afforded the same rights as the client unless otherwise specified by state or federal law, in accordance with the DHHS Privacy Policies.

Documentation required by the HIPAA privacy rule throughout this policy shall be retained at least six (6) years from the date of its creation.

DHHS covered health care components and internal business associates shall negotiate the procedures for complying with this policy.

Right to Confidential Communications

Client Right - Each client of a DHHS agency has a right to request confidential communications by requesting that the agency contact him/her at a different location or by a different means when the agency needs to communicate with the client.

Agency Responsibility - Each DHHS covered health care **provider** must establish accommodations for their clients, whose privacy is not assured in their daily lives, to request alternative means of communication about their health information. Such accommodations may include an alternative location and/or method of contact such as mail, e-mail, fax, or telephone. Covered providers must develop procedures for making reasonable efforts to comply with such requests from their clients; however, providers may not require an explanation from their clients regarding the basis for such request.

Each DHHS covered health **plan** must permit plan recipients to request to receive communications regarding health information from the health plan by alternate means or at alternate locations when requested by a plan recipient. The health plan must accommodate such requests by plan recipients if the request is deemed reasonable. The health plan may require plan recipients to clearly state that the disclosure of all or part of their health information, using the current communication method or location, could endanger the plan recipient.

Client Requests

Each DHHS agency may determine whether or not to require such requests from clients to be in writing, or whether the agency will accept verbal requests. Verbal requests must be documented. The client must specify his/her preferred alternative means or location; and the agreement reached by the client and the agency must be documented.

Agency Assurance

Internal procedures must be developed so all workforce members who are engaging in communications with a client who has requested and received an agreement to use alternative means of communication are aware of the need to use other agreed upon channels in order to protect the client. An agency could face serious liability if a client was harmed due to failure of staff to follow the agency's agreement to use alternative communications.

DHHS agencies must develop procedures that address the following processes for processing confidential communication requests.

- Establishing how the requests will be submitted (orally or writing). Identifying who in the agency is responsible for reviewing the request to decide if it will be accepted.
- Establishing the process to notify the client of the agency's response to the request.
- Establishing the process to document the alternate means of communication.
- Identifying methods to be used to communicate changes to affected staff.
- Ensuring future communications are consistent with the agreement.

Right to Adequate Notice of Use and Disclosure of Individually Identifiable Health Information

Clients of DHHS agencies have a right to be informed about how the agency may use and/or disclose their health information, as well as their rights and the agency's legal duties with respect to protecting the privacy of health information in their possession.

Each DHHS covered health care component must make their *notice of privacy practices* available to their clients, which explains how the component may use and/or disclose their individually identifying health information. This *notice* also describes the rights of clients to take action and the component's legal duties, with regard to the use and/or disclosure of individually identifiable health information created and/or maintained by the agency. The following situations included in each agency's *notice* directly affect client rights.

In an emergency treatment situation, the client has a right for the *notice* to be provided as soon as practicable after the emergency;

- Clients must be assured that whenever there is a material change in the agency's privacy practices, the agency will promptly revise and post their notice of privacy practices. Such changes shall not be implemented prior to the effective date of the revised notice, except as required by law; and
- Health Plan recipients must be assured that whenever a material change has been made to the health plan's notice, the plan will provide a revised notice within 60 days of the revision.

DHHS agencies must establish procedures for ensuring clients' right to adequate notice of the agency's privacy practices. The required procedures listed below directly affect client rights.

- Establish procedures that ensure clients are provided the agency's notice;
- Establish procedures that ensure existing health plan recipients are provided the Plan's notice by April 14, 2003, and thereafter at the time of enrollment;
- Determine who is responsible for ensuring the notice given to clients is current, that revisions are made timely, that the notice is prominently displayed in the agency when required and that the notice is distributed according to the agency's requirements;
- Establish procedures for obtaining written acknowledgement from the client or the client's personal representative of receipt of the covered health care provider's notice, including the agency's good faith efforts if written acknowledgement is not obtained; and
- Establish procedures to follow-up in emergency circumstances wherein the notice was not provided to a client.

Right to Obtain Paper Copy after Electronic Notice

Each client of a DHHS agency may be given the opportunity to receive the agency's *notice of privacy practices* electronically; however, the client further has the right to request that a paper *notice* also be provided.

Each agency may offer to provide its *notice of privacy practices* to agency clients by e-mail, if the client agrees. Any client who receives the *notice* electronically retains the right to obtain a paper copy upon request.

DHHS agencies must develop procedures that address providing clients with a paper copy of the agency's *notice*.

- Establish procedures to ensure clients are provided the agency's notice, including paper and electronic methods.
- Enforce the clients' right to be provided a paper notice, upon request.

- Establish a process for covered health care providers with a direct treatment relationship to clients to obtain written acknowledgement of receipt of the notice, including good faith efforts associated with electronic notice.

Right to Request Access to Individually Identifiable Health Information

Each client of a DHHS agency has the right to request access to inspect and obtain a copy of his/her health information for as long as the information is maintained by the agency in a designated record set. If the agency does not maintain the health information that is the subject of the client's request for access, but knows where the requested information is maintained, the agency must inform the client where to direct his/her request for access.

Each client's request for access to his/her personal health information must be in writing. DHHS agencies may require the requester to:

- Complete agency form for request;
- Submit own written request; or
- Submit electronic request via e-mail.

The client's right to request access to records applies only to those records that have been identified as a 'designated record set'. If the same information requested by the client or personal representative is contained in multiple designated record sets, the agency can limit access to a single designated record set.

DHHS agencies must determine the process for addressing a client's request to access, inspect, and copy his/her records. All requests from clients or their personal representative must be in writing and forwarded to the agency's privacy official, or other designee, who is responsible for ensuring the request is processed in a timely manner, not to exceed 30 days (with a one-time 30 day extension if the record cannot be accessed within the original 30 days). The agency is required to notify the requester in writing of any extension outlining the reasons for the delay.

DHHS agencies must grant access to individually identifiable health information in designated record sets unless it is determined there may be grounds for denial. When access is granted, agencies may provide a summary of the client's record in lieu of the entire record, if that is agreeable with the client and the client agrees in advance to any fees imposed by the agency for producing the summary.

Note: DMH/DD/SAS General Statutes require that client access be determined by an attending physician. If there is not an attending physician, access must be determined by the agency director or his/her designee.

A licensed health care professional may deny access to information in certain circumstances:

- If it is believed such access is reasonably likely to endanger the life or physical safety of the client or another person;

- If the information makes reference to another person (other than a health care provider) and access may cause substantial harm to that person; or
- If the access is requested by the client's personal representative and access could cause substantial harm to the client or to another person.

If access to health information is denied in whole or in part, the licensed health care professional is required to comply with the requirements listed below.

- Determine if access to any other requested information in the designated record set should be allowed.
- Provide the client and the agency's privacy official with a written explanation as to the reason for the denial, that includes:
 - The basis for the denial;
 - If applicable, a statement of the client's review rights; and
 - A description of how the client may complain to the agency, including the name or title and telephone number of the person to contact.

If a client requests review of the denial to access individually identifiable health information, the agency must designate a different licensed health care professional who was not directly involved in the original denial, as a reviewing official to review, within a reasonable period of time, the decision to deny access. The agency must promptly provide written notice to the client of the determination made by the reviewing official. Agencies are required to respond to the request in accordance with the reviewing official's decision.

DHHS agencies may deny access to specific health information, as listed below, without providing a client an opportunity for review:

- Psychotherapy notes;
- Information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding;
- Health information maintained by covered health care components that is subject to the Clinical Laboratory Improvements Amendments of 1988;
- Information created or obtained in the course of research that includes treatment may be temporarily suspended for as long as the research is in progress, provided the client was previously informed of the suspension and consents to it;
- Access to records that are subject to the Privacy Act, 5 U.S.C. 552a may be denied if the denial of access would meet the requirements of that Act; and
- Individually identifiable health information that was obtained from someone other than a health care provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

Each client who has been granted access to review his/her health information also has the right to request a copy of all or part of the health information to which access was granted.

If a client requests a copy of his/her health information or agrees to receive a summary or explanation of such information, DHHS agencies may impose a reasonable, cost-based fee, provided that the fee includes only the cost of:

- Copying, including the cost of supplies for and labor of copying the information;
- Preparation of an explanation or summary of the health information, if receipt of an explanation or summary is agreed to by the requester; and
- Postage, when the individual has requested that the copy, summary, or explanation be mailed.

Note: DMH/DD/SAS agencies are bound by 10 NCAC 18D.0121 when determining fees for copying health information.

Right to Request Amendment to Individually Identifiable Health Information

Each client of a DHHS agency has the right to request amendment of his/her health information that is contained in a designated record set, for as long as the information is maintained in the designated record set. Amendments may include changing or adding information.

Each client's request for amendment to his/her personal health information must be in writing and must include the reason for requesting amendment. Agencies may require the requester to submit the request as follows:

- Complete agency form for amendment;
- Submit own written request; or
- Submit electronic request via e-mail if e-mail is available to the client.

DHHS agencies must document the titles of the persons or the offices responsible for receiving and processing requests for amendments by clients. Such documentation must be retained for at least six (6) years from the date of creation.

DHHS agencies must act on a client's request for amendment no later than 60 days after receipt of the request. If the agency grants the amendment in whole or in part, the following steps must be taken:

- Identify all documents in the designated record set(s) that need(s) to be amended (Note: If the amended information is contained in multiple designated record sets, the amendment must be documented in each record set);
- Allow insertion of the amendment as an addendum to the contested portion of the designated record set; however, the original portion of the designated record set may not be deleted;
- Inform the requester that the amendment is accepted and obtain the client's identification of, and agreement to have the agency notify the relevant persons with which the amendment needs to be shared; and
- Make reasonable efforts to inform and provide the amendment within a reasonable time to those identified by the client and to any business associates who have copies of the health information being amended.

DHHS agencies may deny a request to amend a client's health information if it determines that the information:

- Was not created by the agency (or that the originator of the information is no longer available to evaluate the request for amendment);
- Is not part of a designated record set;
- Is excluded from the information to which a client may request access; or
- Is accurate and complete.

DHHS agencies must provide a timely, written denial to a client that is written in plain language and contains the following elements:

- The basis for the denial;
- The client's right to submit a written statement disagreeing with the denial and how the client may file such a statement;
- A statement that if the client does not submit a statement of disagreement, the client may request that the agency include the client's request for amendment and the denial with any future disclosures of the health information that is the subject of the amendment; and
- Description of procedures to file a complaint. Such description must include the name or title and telephone number of the contact person or designated office.

DHHS agencies must permit a client to submit to the agency a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement. The agency may reasonably limit the length of a statement of disagreement.

DHHS agencies may prepare a written rebuttal to the client's statement of disagreement. Whenever such rebuttal is prepared, the agency must provide a copy to the client who submitted the statement of disagreement.

DHHS agencies must, as appropriate, identify the health information in the designated record set that is the subject of the disputed amendment and append or otherwise link the following to the designated record set:

- The client's request for amendment;
- The agency's denial of the request,
- The client's statement of disagreement with the request denial, if any; and
- The agency's rebuttal to a client's statement of disagreement with a request denial,

If a client has submitted a statement of disagreement, the agency must include the appended material in the designated record set in accordance with the record keeping section above, or at the discretion of the agency, an accurate summary of such information, with any subsequent disclosure of the health information to which the disagreement relates.

If a client has not submitted a written statement of disagreement, the agency must include the client's request for amendment and its denial, or an accurate summary of such information, with any subsequent disclosure of the health information only if the client has requested such action.

When a subsequent disclosure described above is made using a standard transaction that does not permit the additional material to be included with the disclosure, the agency may separately transmit the required material to the recipient of the standard transaction.

DHHS agencies that are informed by other agencies/components of an amendment to a client's health information must also amend the health information in its own designated record sets.

Documentation of requested amendments and the disposition of such requests shall be retained for at least six (6) years from the date of its creation or the date when it was last in effect, whichever is later. Documentation that is maintained in the client record shall be retained in accordance with the General Schedule for State Agency Records.

DHHS agencies must develop the following procedures to address when clients request amendments to their health information.

- Designating the persons or offices responsible for receiving and processing requests for amendment by clients;
- Identifying reviewing official(s);
- Developing a request form, if applicable;
- Developing guidelines for establishing response time;
- Establishing criteria to be used in determining acceptance or non-acceptance of requested amendment;
- Defining methods for processing amendments of paper and electronic records;
- Establishing process for notifying requester of decision;
- Establishing process for making reasonable efforts to provide amendment to persons identified by the client and any other persons, including business associates, that the agency knows has been provided health information that is the subject of an amendment, within 60 days of the date of the amendment; and
- Establishing process so that the billing is reviewed to see if it should be amended or changed to reflect the new information when the amendment affects a service for which billing or charges have already been submitted.

Right to Accounting of Disclosures of Individually Identifiable Health Information

Each client of a DHHS agency has a right to receive an accounting of disclosures of his/her health information made by the agency at any time during the previous six (6) years. Such requests may not include dates prior to April 14, 2003. This includes any disclosures made to or by any business associate of the agency. Disclosures made as follows do not have to be included on an accounting of disclosures:

- Disclosures to the client;

- Disclosures made based upon signed authorization of the client or personal representative; or
- Disclosures for purposes of treatment, payment or health care operations.

Disclosures made to health oversight agencies or law enforcement officials may be temporarily excluded from an accounting if the covered agency has been notified by the oversight agency or law enforcement official that providing an accounting could impede the progress of their activities.

DHHS agencies shall require requests for accounting of disclosures to be in writing and forwarded to designated staff for action. Agencies are required to act on such requests within 60 days after receipt of the request, unless there is good reason to extend the time to reply by another 30 days. Any extension requires the agency to provide a written statement to the requester regarding the reason for the delay and the expected completion date. Only one (1) extension is permitted per request.

The DHHS Privacy Policy, *Client Rights Policies*, *Accounting of Disclosures* provides all the requirements DHHS agencies must follow.

For purposes of this policy, agencies must be familiar with the following basic information for each disclosure that is required to be tracked and would therefore be available to a client upon request:

- Date of disclosure;
- Name of covered entity or individual who received the information (and their address, if known);
- Description of information disclosed; and
- Brief statement of the purpose or reason for the disclosure.

DHHS agencies must provide clients or their personal representatives the first accounting of disclosures free of charge in any 12-month period. Agencies may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same individual within the same 12-month period, provided that the agency informs the client in advance of the fee and provides the client with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee. (Refer to DHHS Privacy Policy, *Client Rights Policies*, *Accounting of Disclosures*.)

DHHS agencies must develop the following procedures to ensure their clients' right to an accounting of disclosures of their health information. (Refer to the DHHS Privacy Policy, *Client Rights Policies*, *Accounting of Disclosures* for detailed requirements for accounting of disclosures.)

- Designating the person(s) or office(s) responsible for receiving and processing requests for accounting of disclosures by clients;
- Identifying reviewing official(s);
- Developing request form, if applicable;
- Developing guidelines for establishing response time;
- Establishing criteria to be used in identifying accountings;
- Establishing process to ensure required disclosures are routinely documented;

- Establishing process for making reasonable efforts to provide accounting to clients within 60 days of request;
- Determining any charges and establishing a basis for making such determinations; and
- Maintaining audit trails that track client requests for accountings.

7. **Right to Request Privacy Restrictions for Individually Identifiable Health Information**

Each client of a DHHS agency has the right to object to, and request restrictions on, how his/her health information is used or to whom the information is disclosed. Clients can make such requests/objections even if the restriction affects the clients' treatment or payment for that treatment or other health care operation activities. Use and disclosure of health information for treatment, payment, or other health care operations is oftentimes permitted by state and/or federal law without the client's authorization or consent. The client may want to limit the health information that is included in any of the following:

- Agency directories;
- Health information that is provided to family or friends who are involved in the client's care;
- Payment of medical bills; or
- Health information that is provided to authorities involved with disaster relief efforts.

DHHS agencies are not required to agree to any requested restrictions. However, if a restriction is agreed to, it is binding and agencies may not use or disclose information in violation of the agreement, unless otherwise allowed or required under other DHHS policies. For example, an agency may disclose restricted information to permit emergency treatment. An agency is also not bound by restrictions when a disclosure is required by law. DHHS agencies are encouraged to require client request for restrictions to be in writing.

DHHS agencies must establish procedures to address the following processes for ensuring clients' right to request privacy restrictions of their health information.

- Designating the person(s) or office(s) responsible for receiving and processing requests for privacy restriction;
- Determining the acceptable method(s) for requesting restriction(s);
- Developing process for taking action on request; and
- Establishing documentation requirements.

Agreement or Denial of a Request for Restriction

DHHS agencies must establish procedures for processing clients' requests for restricting the use and/or disclosure of their health information, including the agency's process when request is agreed to and when request is denied. Procedures must ensure client's request is processed within 60 days of the request and client is fully informed of the decision.

If the restriction is agreed to, the following procedure must be implemented:

- The agency must honor the restriction;
- The restriction must be communicated to the agency staff in an approved manner; and
- Documentation of the approved request must be provided to the client.

If the request for restriction is denied, the following procedure must be implemented:

- The agency's denial of the request shall be documented according to agency requirements and
- Documentation of the denied request must be provided to the client.

DHHS agencies may terminate an agreement to a restriction at any time. If the client agrees to the termination by the agency, previously restricted information may be used or disclosed as if a restriction never existed. If a client objects to the termination, the termination is still in effect, but only with respect to the health information created or received after the client is informed of the termination of the restriction.

DHHS agencies must develop procedures that address the following processes for terminating a client-requested privacy restriction.

- Documentation of written or oral agreement must be maintained;
- The agency must inform the client that it is terminating its agreement to a restriction and that such termination is only effective with respect to health information created or received after it has so informed the client;
- Subsequently, the restriction shall be removed, and such action shall be documented; and
- Any documentation that alerted staff to the restriction must be removed (e.g., any "flag" in records/forms, etc).

If a DHHS agency has agreed to a restriction but the client who requested the restriction is in need of emergency treatment and the restricted health information is needed to provide the emergency treatment, the agency may disclose the health information to a health care provider to provide such treatment.

If such health information is disclosed in an emergency situation, the agency must inform the health care provider to whom the information was disclosed not to further use or disclose that health information.

DHHS agencies must address the following processes when allowing clients to request restrictions on the use and/or disclosure of their health information.

- Designating the person or office responsible for receiving and processing requests for restricting use/disclosures by clients;
- Developing restriction request form, if applicable;
- Developing guidelines for establishing response time;
- Establishing criteria to be used in approving/denying restrictions;
- Establishing process to ensure all restrictions are documented timely;

- Establishing procedures to inform agency staff of approved restrictions, as well as termination of restrictions; and
- Identifying documentation requirements to support all the above decisions.

Each client of a DHHS agency has the right to submit a complaint if he/she believes that an agency within DHHS has improperly used or disclosed his/her individually identifiable health information, or if a client has concerns about the privacy policies of DHHS or concerns about DHHS compliance with such policies.

Each agency is required to identify a person or office in the agency that clients may contact if they have questions or concerns about the agency's privacy policies and procedures, or if clients would like to submit a complaint regarding the use and disclosure of their health information.

DHHS agencies must provide a process for clients to submit a complaint for any of the following reasons:

- If they feel their privacy rights have been violated;
- If they want to file complaints about the agency's privacy policies and procedures; and/or
- If they want to file a complaint about the agency's compliance with their privacy policies and procedures.

Such process shall ensure no retaliation may be taken against a client for filing a complaint against the agency.

DHHS agencies are also required to inform clients of a contact in the U.S. Department of Health and Human Services should they wish to submit a complaint to that level. Agencies are required to include this information in their *Notice of Privacy Practices*.

DHHS agencies must develop procedures that address the following processes when ensuring clients' right to submit complaints about the agency's privacy policies and procedures or about the agency's use and disclosure of their health information.

Designating the person(s) or offices(s) responsible for receiving and processing complaints submitted by clients;

- Identifying agency contact person;
- Determining acceptable method(s) for receiving complaints;
- Developing complaint form, if applicable;
- Developing guidelines for establishing response time;
- Establishing criteria to be used in reviewing complaints;
- Establishing protocols for addressing complaints;
- Identifying persons involved in disposition of complaint;
- Establish procedures for resolving complaints; and
- Identifying documentation requirements to support all decisions.

CHAPTER TWENTY : Personal Representatives

DHHS agencies shall recognize personal representatives who are authorized by the courts or by state or federal law to act on behalf of clients regarding their individually identifying health information in a manner consistent with all requirements within this policy. DHHS agencies shall treat the personal representative as the client with regard to the client's individually identifying health information relevant to the matters on which the personal representative is authorized to represent the client.

In most situations, clients are authorized to make health care decisions on their own behalf and do not require a personal representative if they are:

- Adults (individuals 18 years of age or older) who have not been adjudicated incompetent;
- Individuals under 18 years of age who are married, serve in the Armed Forces of the United States, or who have been declared emancipated by a court of competent jurisdiction;

A personal representative is usually required to make health care decisions about adults adjudicated incompetent and persons under 18 years of age (unless they meet the exception noted above).

Personal representatives may include the following:

- Person ordered by the court;
- Parent(s), of juveniles under 18 years of age;
- Person, other than parent, acting in loco parentis (of minor);
- Guardian as defined in chapter 35A;
- Person with health care power of attorney. The health care power of attorney document should define the scope of the personal representation with respect to access to individually identifying health information. The individual may also be referred to "health care agent" or "health care attorney-in-fact"; or
- Executor/administrator of estate (of deceased person)

Disclosure of individually identifying health information to a personal representative is required (with the exception of those situations described in this policy) only if disclosure to the client is required.

Generally, a parent, guardian, or other person acting *in loco parentis* who has the authority to make health-related decisions on behalf of a client who is an unemancipated minor must be treated as a personal representative and may access and control health information about the minor.

The minor may control his/her health information related to a particular service and exercise the privacy rights afforded to the client in any of the following circumstances:

- If the parent, guardian or other person acting in loco parentis has agreed to a confidential relationship between the minor and the physician for a particular health care service;
- Where a minor can obtain a particular health care service under their own consent (for example, as specified in NCGS 90-21.5), and no other consent is required by law (regardless of whether such consent has actually been obtained), the parent, guardian or other person acting in loco parentis may not be treated as the personal representative, unless the minor requests they be treated as such;
- If the minor may lawfully obtain care without consent of a parent, guardian or person acting in loco parentis, and the minor, a court, or another person authorized by law consents to the service (for example, as specified in NCGS 90-21.7), the parent, guardian or person acting in loco parentis may not be treated as the personal representative; or
- In DHHS agencies under the Division of Mental Health, Developmental Disabilities and Substance Abuse Services, both the minor and parent, guardian or person acting in loco parentis must authorize disclosure of the minor's health information when either of the following applies:
 - In agencies designated as 'substance abuse programs' under 42 CFR Part 2, when the minor's parent or guardian has consented to the minor's treatment for substance abuse; or
 - When disclosures are made to external client advocates.

In the case of joint parental custody, either parent may be treated as the personal representative of the minor unless a court order dictates otherwise.

Disclosure of health information about a minor to a parent, guardian or person acting *in loco parentis* to avert a serious and imminent threat to the health or safety of the minor is permitted even if the minor obtained the health service without the consent of the parent, guardian, or person acting *in loco parentis*.

Any individual who has legal authority to act on behalf of an adult or to act on behalf of an emancipated minor who has been determined to lack the capacity to make health-related decisions, shall be treated as a personal representative as it relates to the client's health information relevant to the matters on which the personal representative is authorized to represent the client.

In the case of shared guardianship, both guardians must be treated as personal representatives and both have equal rights regarding decisions related to the client's individually identifying health information. Both guardians must signify agreement in order to execute a decision, unless a court order dictates otherwise.

An executor, administrator, or other person who has authority to act on behalf of a deceased client or of the client's estate shall be recognized as the personal representative with respect to the deceased client's individually identifying health information. The next of kin of a deceased individual can be treated as the personal representative when there is no executor or administrator.

The following persons, in priority order, can be treated as the personal representative of a deceased individual with respect to authorizing anatomical gifts/organ donations and the individually identifying information pertaining to the making of the anatomical gift/organ donation:

- Spouse;
- Adult child;
- Either of the individual's parents;
- Adult sibling;
- Guardian of the person;
- Any other person authorized or under obligation to dispose of the body.

An agency may disclose individually identifying health information to a funeral director as necessary to carry out their duties with respect to the decedent.

An agency may decide not to treat an individual as a personal representative of the client if, in the exercise of professional judgment, the agency determines that it is not in the best interest of the client to treat the individual as the client's personal representative, and that either of the following exists:

- The covered entity has a reasonable belief that the client has been or may be subjected to domestic violence, abuse, or neglect by such person; or
- That treating such person as the personal representative could endanger the client.

If the client is present for, or otherwise available prior to a disclosure, the agency may disclose to a family member(s) or friend(s) individually identifying health information that is directly relevant to that person's involvement with the client's health care if the agency meets one of the following criteria:

- Obtains the client's authorization to disclose to the parties involved in their care;
- Provides the client with the opportunity to object to the disclosure, and the client does not object (this provision does not apply to DHHS agencies under the Division of Mental Health, Developmental Disabilities and Substance Abuse Services); or
- Reasonably infers from the circumstances, based on professional judgement that the client does not object to the disclosure.

If the client is not present for the disclosure, or the opportunity to agree or object to the use or disclosure cannot practicably be provided because of the client's incapacity or an emergency circumstance, the agency may use professional judgment to determine whether the disclosure is in the best interest of the client. If so, the agency may disclose only the health information that is directly relevant to the family member/friend's involvement with the client's health care.

An agency may use professional judgment and experience with common practice to make reasonable inferences of the client's best interest in allowing a person to act on behalf of the client to pick up filled prescriptions, medical supplies, x-rays, or other similar forms of individually identifying health information.

An agency may disclose the necessary individually identifying health information to notify or assist in the notification of family members, personal representatives, or other persons responsible for a client's care with respect to a client's location, condition, or death.

Each DHHS agency shall develop and implement procedures for determining who qualifies as a personal representative. These procedures shall include the identification of persons in the agency who are responsible for confirming the legal status of each individual identified as a personal representative of a client.

The personal representative's name, address and relationship to the client shall be documented in the client's record so that all staff are aware of who is authorized to approve or deny the use and/or disclosure of the client's individually identifying health information. Documentation should also include the name of the staff member confirming the legal status of the personal representative and the date that such legal status of the personal representative was determined.

Procedures shall be developed and implemented that outline steps to be taken should the agency be unable to recognize an individual as a personal representative.

CHAPTER TWENTY TWO: DESIGNATED RECORD SETS

DHHS agencies shall identify categories of records maintained, collected, used, or disseminated by the agency that contain individually identifiable health information including medical records and billing records maintained by health care providers, specified records maintained by health plans and other records used in making decisions about clients.

Such records shall be termed "Designated Record Sets" and shall be considered the only personal health information records to which clients have a right to request access, amendment, and copies.

A Designated Record Set is a description of health and/or business information that can be maintained in one or many areas within an agency.

The term *record* means any item, collection, or grouping of information that includes information (including individually identifiable health information) and is maintained, collected, used, or disseminated by or for a health plan or health care provider.

Designated Record Sets are maintained by or for a health plan or health care provider and include:

- Medical records and billing records of individual clients, maintained by or for a covered health care provider;
- Employee health records that are maintained separately from personnel records;
- The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
- Categories of records that are used, in whole or in part, to make decisions about clients.

Records created and/or maintained by an External Business Associate for services rendered to a DHHS agency must be considered when evaluating documentation for Designated Record Sets.

It is the responsibility of each DHHS agency to ensure that a Business Associate Agreement is in place when required.

Health information specifically created and/or maintained by External Business Associates, when acting on behalf of a DHHS agency, is subject to the client rights provisions to request access to or amendment of such information in accordance with the Business Associate Agreement. Copies of information that are also maintained by a health care provider or health care plan should not be included in the Business Associate's Designated Record Set.

DHHS agencies are **not required** to allow clients access to Designated Record Sets if a licensed health care professional determines that access to such information would not be in the best interest of the client or another individual, and such determination is documented.

DHHS agencies are **not required** to amend, at a client's request, any information in a record that the agency knows to be true and accurate.

Internal Business Associates who maintain individually identifiable health information are subject to the requirements of this policy in identifying Designated Record Sets. This is accomplished by joint agreement of the DHHS agency and its Internal Business Associate(s).

A process must be developed to evaluate the documentation maintained by the agency to determine those groups of records that should be categorized as Designated Record Sets. The defined process should ensure that the following information is gathered about the evaluated records:

- Documentation type (e.g., medical record)
- Basic content (e.g., assessments, reports, examinations)
- Location of the documentation (e.g., Medical Record Department)
- Contact person (e.g., agency privacy official)
- Paper/electronic documentation (e.g., paper)
- Documentation contains individually identifiable information (e.g., yes)
- Documentation is used to make decisions about the client (e.g., yes)

The first step in the implementation of Designated Record Sets that are to be made available to clients is to identify and assess those health information records within the agency that may be classified as a Designated Record Set.

Identifying categories of Designated Record Sets requires an assessment of all documentation to determine which records should be included or excluded before further consideration is given to the categories to be classified as Designated Record Sets.

Documentation requirements must be assessed in order to identify those records that meet the intent of this policy. Health information in all types of media (e.g., paper, oral, video, electronic, film, digital) must be considered. Minimally, the following categories of records should be considered Designated Record Sets:

Medical Records

- Identify what constitutes the medical records in your agency (e.g., paper records stored in medical record folders maintained in the Health Information Management Department; active medical records utilized by health care staff prior to client discharge).
- If the agency uses an electronic medical record for all or parts of the medical record, specify if the Designated Record Set is the automated system or a copy produced from the automated system.

- Specify if copies of records from other health care providers will be included as part of the Medical Record Designated Record Set.

Copies may be included as part of the Designated Record Set for access only; clients may be required to go to the source of the information to request amendments.

Business Records

Specify if the Designated Record Set is an automated system or a hard copy report produced by an automated system for the following:

- Eligibility information maintained by health plans
- Enrollment records maintained by health plans
- Claims records submitted to or received from health plans
- Remittance Advices and records of payments
- Patient Statements
- Claims adjudication records
- Case or medical management records maintained by health plans

Other records used by health plans and health care providers **to make decisions about individuals**. For example, documentation such as raw test data and laboratory reports maintained by various programs in the agency are considered "working records" and should be evaluated as to the benefit to clients to request access and amendment. Reports developed from working records that are filed in the medical record should be evaluated with the medical record as a whole and not as separate documentation. Examples of working records may include:

- Raw test data from psychological tests
- Audio tapes (e.g., dictation tapes, taped sessions with clients/family that would not be considered psychotherapy notes)
- Psychotherapy note
- Videos/photographs of clients used for teaching purposes
- Telemedicine
- Coding worksheets
- Utilization review worksheets
- X-ray film
- Working notes summarized and dictated into the client record

Exclusions

- Health information that is not used to make decisions about individuals should not be included in a Designated Record Set. Such information may be found in many types of records that

include significant information not relevant to the client, as well as information about other persons.

- Some records (e.g., administrative records, oversight records) that are maintained by the agency require independent evaluation to determine whether or not they should be considered a Designated Record Set, such as:

1. Quality Improvement records

- Risk Management records (including Incident Reports)
- Copies of reports/documentation/forms already designated
- Cancer Registry information
- Research documentation
- Education records governed by Family Educational Rights Privacy Act (FERPA)

Documentation must be maintained that supports the agency's assessment of its records for determination of its Designated Record Sets. Documentation may be maintained electronically or on paper.

Such information must be kept current and available for reference should a client request access to his/her health information, including comments that identify any information included in a Designated Record Set that the client would not have a right of access, amendment, or copies.

Documentation requirements must be maintained for a period of at least six (6) y

CHAPTER TWENTY-FIVE: ACCEPTABLE USE FOR DHHS INFORMATION SYSTEM

Each DHHS Division/Office shall be responsible for ensuring that every individual seeking access to DHHS network and/or information systems reviews this policy and signs an acceptable use agreement based upon the terms specified in this policy. Users must sign the agreement form included herein before permission is granted to use the DHHS systems.

All information and data processing systems to which users are given access are to be used only to conduct the activities authorized by the department. The use of these resources must be conducted according to the policies, standards, and procedures instituted by the department or on its behalf. The unauthorized use or disclosure of information provided by these data processing systems may constitute a violation of department, state, and/or federal laws which will result in disciplinary action consistent with the policies and procedures of the department (see **Enforcement** section below).

DHHS Divisions/Offices may require additional agreements regarding the confidentiality of specific types of information; for example, medical records, client case files, personnel records, financial records, etc. This policy may augment such division/office policies, but is not intended to replace such policies, which remain in effect.

The department and its divisions/offices retain the rights of ownership to all ITS resources including hardware, software, functionality, data, and related documentation developed by the department's information systems users on behalf of the department. All department IS resources remain the exclusive property of the State of North Carolina (NC) and/or the department, unless otherwise prescribed by other contractual agreements.

The Internet is a world-wide collection of interconnected computer networks. The state's wide area network, NCIIN, is the NC controlled network connected to the Internet.

Following is a list of policies regarding the use of NCIIN and the Internet:

- While in performance of work-related functions, while on the job, or while using publicly owned or provided information processing resources, DHHS users are expected to use the NCIIN and Internet responsibly and professionally. Users shall make no intentional use of these services in an illegal, malicious, or obscene manner as described in NC General Statute (GS) 14-190.1. Users may make reasonable personal use of publicly owned or provided NCIIN or Internet resources as long as:

- The direct measurable cost to the public is none, is negligible, or access supports the mission of the agency;
- There is no negative impact on user's performance of public duties;
- The policy is applied equitably among all personnel of the agency;
- Users may be required to reimburse the agency if costs are incurred that do not have prior approval by the agency or division/office.
- When sending or forwarding e-mail over the NCIIN or the Internet, users shall identify themselves clearly and accurately. Anonymous or pseudonymous posting is expressly forbidden, unless otherwise allowed by law to make anonymous postings.

Users are responsible for protecting DHHS sensitive information by following the DHHS policies and DHHS division/office policies and procedures.

Users have a responsibility to ensure, to the best of their ability, that all public information disseminated via NCIIN and the Internet is accurate. Users shall provide in association with such information the date at which it was current and an e-mail address allowing the recipient to contact the public staff responsible for making the information available in its current form.

Users shall avoid unnecessary network traffic and interference with other users, including but not limited to:

- Unsolicited commercial advertising by DHHS Users. Such use is strictly forbidden. For the purpose of this policy, "unsolicited commercial advertising" includes any transmission that describes goods, products, or services and that is initiated by a vendor, provider, retailer, or manufacturer of the described goods, products or services, or by a third party retained by, affiliated with, or related to the vendor, provider, retailer, or manufacturer. For purposes of this definition the vendor, provider, retailer, or manufacturer must be a non-governmental entity. This prohibition shall not include:
 - Discussions of a product or service's relative advantages and disadvantages by users of those products or services (unless the user is also the vendor, retailer or manufacturer, or related or affiliated with the vendor, provider, retailer, or manufacturer),
 - Responses to questions, but only if such responses are direct replies to those who inquired via e-mail, or
 - Mailings to individuals or entities on a mailing list so long as the individual or entity voluntarily placed his/her name on the mailing list.
 - The use of computer resources, including e-mail, to conduct any activities already prohibited by the Office of State Personnel or other DHHS policies (such as private/personal fund raising, political activities, etc.) shall be prohibited.
 - Mass emailing by public employees and NCIIN users that do not pertain to governmental business is prohibited.

- Users shall not use the Internet, the NCIIN, or any state information system to (i) allow the unauthorized dissemination of confidential information, or (ii) for any purpose that is not permitted by DHHS policies or would compromise public safety or public health.
- Users shall not stalk others; post, transmit, or originate any unlawful, threatening, abusive, fraudulent, hateful, defamatory, obscene, or pornographic communication, or any communication where the message, or its transmission or distribution, would constitute a criminal offense, a civil liability, or violation of any applicable law.
- Users shall not access or attempt to gain access to any computer account to which they are not authorized. They shall not access or attempt to access any portions of the NCIIN networks to which they are not authorized. Users also shall not intercept or attempt to intercept data transmissions of any kind to which they are not authorized.
- Users given access to which they are not privileged or entitled, are required to report the circumstances immediately to their supervisor. Supervisors are responsible for determining the User's appropriate access rights. Supervisors must notify their division/office information security official should they determine that access rights need to be modified.

Workstation Security

These requirements apply to office, home or other remote access locations if utilized for DHHS business.

- As appropriate, sensitive paper and computer media shall be stored in suitable locked cabinets and/or other forms of security furniture when not in use, or behind locked doors, especially outside working hours.
- Personal computers and computer terminals should not be left logged on when unattended or not in use. Personal computers or computer terminals shall be protected from unauthorized access by physical, technical, or administrative controls such as passwords, time driven screensavers, controlled workstation access, operational procedures, etc
- Classified or sensitive information should not be printed on a printer located in public areas. However, in the event that public printers must be used to print sensitive or classified information, such information shall be cleared from printers immediately.

Classified information stored on external media (e.g., diskettes or CDs) must be protected from theft and unauthorized access. Such media must be appropriately labeled so as to identify it as classified information.

The use of removable storage devices or external devices (e.g., USB Flash Drives) shall be restricted to authorized personnel in order to safeguard and protect confidential data and information technology assets. Authorization for the use of removable storage devices must be granted by the user's supervisor in writing and specify the intended use of the device. The division/office security official shall maintain an inventory of all authorizations and use of removable storage devices. Any use must meet DHHS security policies and standards.

Users shall request the use of state owned storage devices. Division/offices shall strive to provide state owned-storage devices to staff and there by limit the use of any personal device used to conduct any state business. Any use of personal devices must be disclosed to the supervisor and be approved.

Mobile computing devices and removable storage devices (e.g., laptops, PDAs, USB flash drives, etc) must never be left in unsecured areas and their use must meet DHHS Security Policies and Standards. Any incidents of misuse, theft or loss of data must be reported to the supervisor and to the division security official. The incident should be reviewed and reported in accordance with the DHHS Incident Management Policy and Procedures.

DHHS sensitive or confidential information shall not be stored at home without appropriate authorization from the user's supervisor/manager, in consultation with the division/office security official. Users shall follow appropriate physical safeguards for offsite use. Documentation of authorization and storage of sensitive information in the home shall be maintained in accordance with the division/office's procedures.

All users of the department's information systems are advised that their use of these systems may be subject to monitoring and filtering. DHHS reserves the right to monitor – randomly and/or systematically – the use of Internet and DHHS information systems connections and traffic. Any activity conducted using the state's information systems (including but not limited to computers, networks, e-mail, etc.) may be monitored, logged, recorded, filtered, archived, or used for any other purposes, pursuant to applicable departmental policies and state and federal laws or rules. The department reserves the right to perform these actions with or without specific notice to the user.

Software License Agreements

- The theft of computer resources, including computer software, is illegal. All computer software, including software obtained from sources outside the department, is subject to license agreements that may restrict the user's right to copy and use the software. Software distributed on a trial basis, even through the Internet, does not suggest that the software is free or that it may be distributed freely.
- The department does not require, request, or condone unauthorized use of computer software by its employees, volunteers, and contractors. The department enforces Federal Public Law 102-561, which strictly prohibits any violation of copyright protection. Violation of copyright protection is considered a felony and is punishable by up to five (5) years in prison and/or fines up to \$250,000 for all parties involved.

Computer Viruses: Malicious Code

It is the responsibility of each user to help prevent the introduction and spread of computer viruses and other malicious code. All personal computers in the department must have virus detection software running at all times. All files received from any unknown source external to the department, including those on storage on media and electronically downloaded or received as e-mail attachments, except for

attachments received via internal mail system, must be scanned for computer viruses before opening or using the files. (Attachments received via internal mail system are automatically scanned.)

Users should immediately contact their manager or supervisor, other appropriate designated staff or the division/office security official when a virus is suspected or detected, so that it may be confirmed and removed by the appropriate staff.

Users must report all information security violations to the division/office security official, who will notify the DHHS Privacy and Security Office in accordance with the DHHS Incident Management Policy and Procedures. The DHHS Security Officer shall be responsible for notification of the ITS Security Office.

Installation of Hardware or Software

DHHS information system hardware and software installations and alterations are handled by authorized DHHS employees or contractors only. Users shall not install new or make changes to existing information system hardware or software.

Users shall not download software from the Internet unless specifically approved by the user's supervisor and the designated IT personnel. Downloading audio or video stream for a work-related webinar or audio conference is permissible without prior authorization.

Remote Access

Authorized users of DHHS's computer systems, networks and data repositories may be permitted to remotely connect to those systems, networks and data repositories to conduct state-related business only. Users will only be granted remote access through secure, authenticated and managed access methods and in accordance with the ITS and DHHS Remote Access Security Policy and Standard.

- A. Users shall not access agency networks via external connections from local or remote locations, including homes, hotel rooms, wireless devices, and off-site offices without knowledge of and compliance with the User Access Responsibilities section described above within this policy.

USER CERTIFICATION OF NOTIFICATION AND AGREEMENT OF COMPUTER USE POLICY

I certify that I am an employee, volunteer, guest, vendor or contractor working for or on behalf of the Department of Health and Human Services and that I have read this "Acceptable Use Policy" and understand my obligations as described herein. I understand that this policy was approved by the Secretary of the Department of Health and Human Services and these obligations are not specific to any individual Division or Office of the Department, but are applicable to all employees, volunteers, and contractors of the Department. I understand that failure to observe and abide by these obligations may result in disciplinary action, which may include dismissal and/or contract termination. I also understand that in some cases, failure to observe and abide by these obligations may result in criminal or other legal

actions. Furthermore, I have been informed that the Department will retain this signed Agreement on file for future reference. A copy of this Agreement shall be maintained in the personnel file and/or in the contract administration file.

Print
Name _____

Employee, Volunteer, Guest, Vendor or Contractor Signature
_____ Date _____

Supervisor's Signature
_____ Date _____
